



# HP 10Gb Ethernet BL-c Switch

## Command Reference Guide

Part number BMD00022  
January 2008



2350 Mission College Blvd.  
Suite 600  
Santa Clara, CA 95054  
[www.bladenetwork.net](http://www.bladenetwork.net)

## Legal notices

© 2007 Blade Network Technologies, Inc.

This document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this document may be reproduced in any form by any means without prior written authorization of Blade Network Technologies, Inc. Documentation is provided "as is" without warranty of any kind, either express or implied, including any kind of implied or express warranty of non-infringement or the implied warranties of merchantability or fitness for a particular purpose.

U.S. Government End Users: This document is provided with a "commercial item" as defined by FAR 2.101 (Oct. 1995) and contains "commercial technical data" and "commercial software documentation" as those terms are used in FAR 12.211-12.212 (Oct. 1995). Government End Users are authorized to use this documentation only in accordance with those rights and restrictions set forth herein, consistent with FAR 12.211- 12.212 (Oct. 1995), DFARS 227.7202 (JUN 1995) and DFARS 252.227-7015 (Nov. 1995).

Blade Network Technologies, Inc. reserves the right to change any products described herein at any time, and without notice. Blade Network Technologies, Inc. assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by Blade Network Technologies, Inc. The use and purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of Blade Network Technologies, Inc.

Microsoft®, Windows®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

SunOS™ and Solaris™ are trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Cisco® is a registered trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

Part number: BMD00022

January 2008

---

# Contents

Command line interface .....	8
Introduction .....	8
Additional references .....	8
Connecting to the switch .....	8
Establishing a console connection .....	9
Setting an IP address .....	9
Establishing a Telnet connection .....	10
Establishing an SSH connection .....	10
Accessing the switch .....	11
Idle timeout .....	12
Typographical conventions .....	13
Menu basics .....	14
Introduction .....	14
Main Menu .....	14
Menu summary .....	14
Global commands .....	15
Command line history and editing .....	17
Command line interface shortcuts .....	18
Command stacking .....	18
Command abbreviation .....	18
Tab completion .....	18
First-time configuration .....	19
Introduction .....	19
Configuring Simple Network Management Protocol support .....	20
Setting passwords .....	20
Changing the default administrator password .....	20
Changing the default user password .....	22
Changing the default operator password .....	22
Information Menu .....	24
Introduction .....	24
Menu overview .....	24
System Information Menu .....	25
SNMPv3 Information Menu .....	26
SNMPv3 dump .....	32
System information .....	33
Show last 100 syslog messages .....	34
System user information .....	35
Layer 2 information .....	36
FDB information menu .....	37
Link Aggregation Control Protocol information .....	38
Hot Links Trigger information .....	39
802.1X information .....	40
Spanning Tree information .....	42
Rapid Spanning Tree / Multiple Spanning Tree information .....	44
Common Internal Spanning Tree information .....	46
Trunk group information .....	48

VLAN information .....	48
Fast Uplink Convergence status .....	49
Layer 3 information .....	50
Route information .....	51
Show all IP Route information .....	51
ARP information .....	53
OSPF information .....	54
Routing Information Protocol information .....	58
IP information .....	59
IGMP multicast group information .....	60
VRRP information .....	62
Server Mobility Port information .....	63
QoS information .....	64
802.1p information .....	64
ACL information .....	65
RMON Information Menu .....	66
RMON history information .....	66
RMON alarm information .....	67
RMON event information .....	68
Link status information .....	69
Port information .....	70
Transceiver status .....	70
Uplink Failure Detection information .....	71
Information dump .....	71
<b>Statistics Menu .....</b>	<b>72</b>
Introduction .....	72
Menu information .....	72
Port Statistics Menu .....	73
802.1X statistics .....	74
Bridging statistics .....	76
Ethernet statistics .....	77
Interface statistics .....	79
Internet Protocol (IP) statistics .....	81
Link statistics .....	81
Port RMON statistics .....	82
Layer 2 statistics .....	84
FDB statistics .....	84
LACP statistics .....	84
Hot Links statistics .....	85
Layer 3 statistics .....	86
GEA Layer 3 statistics menu .....	87
IP statistics .....	88
ARP statistics .....	89
DNS statistics .....	89
ICMP statistics .....	90
TCP statistics .....	91
UDP statistics .....	93
IGMP Multicast Group statistics .....	93
OSPF statistics menu .....	94
VRRP statistics .....	98
RIP statistics .....	99
Management Processor statistics .....	100
Packet statistics .....	100

TCP statistics .....	101
UDP statistics .....	101
CPU statistics .....	102
Access Control List (ACL) statistics menu .....	102
ACL statistics .....	102
SNMP statistics .....	103
NTP statistics .....	105
Uplink Failure Detection statistics .....	106
Statistics dump .....	107
<b>Configuration Menu .....</b>	<b>108</b>
Introduction .....	108
Menu information .....	108
Viewing, applying, reverting, and saving changes .....	109
Viewing pending changes .....	109
Applying pending changes .....	109
Reverting changes .....	109
Saving the configuration .....	110
Reminders .....	110
System configuration .....	111
System host log configuration .....	112
Secure Shell Server configuration .....	114
RADIUS server configuration .....	115
TACACS+ server configuration .....	116
NTP server configuration .....	118
System SNMP configuration .....	119
SNMPv3 configuration .....	120
System Access configuration .....	127
Port configuration .....	131
Temporarily disabling a port .....	132
Port link configuration .....	132
Port ACL/QoS configuration .....	133
Port PVRST configuration .....	134
Layer 2 configuration .....	135
802.1X configuration .....	136
Rapid Spanning Tree Protocol/ Multiple Spanning Tree Protocol configuration .....	140
Common Internal Spanning Tree configuration .....	141
Spanning Tree configuration .....	144
Forwarding Database configuration .....	148
Static FDB configuration .....	148
Trunk configuration .....	149
IP Trunk Hash configuration .....	150
Link Aggregation Control Protocol configuration .....	151
VLAN configuration .....	152
Protocol VLAN configuration .....	153
Private VLAN configuration .....	154
Hot Links configuration .....	155
Layer 3 configuration .....	158
IP interface configuration .....	159
Default Gateway configuration .....	160
IP Static Route configuration .....	161
Address Resolution Protocol configuration .....	161
Static ARP configuration .....	162
IP Forwarding configuration .....	162

Network Filter configuration .....	163
Route Map configuration.....	163
IP Access List configuration.....	164
Routing Information Protocol configuration.....	165
Open Shortest Path First configuration .....	168
OSPF Interface configuration .....	170
IGMP configuration .....	175
Domain Name System configuration.....	180
Bootstrap Protocol Relay configuration .....	180
Server Mobility configuration.....	181
Virtual Router Redundancy Protocol configuration.....	183
Quality of Service configuration.....	190
QoS 802.1p configuration.....	190
Access Control configuration .....	191
Access Control List configuration .....	191
ACL Ethernet Filter configuration .....	192
ACL IP Version 4 Filter configuration.....	193
ACL TCP/UDP Filter configuration .....	194
ACL Meter configuration .....	195
ACL Re-mark configuration .....	195
ACL Packet Format configuration.....	197
ACL Group configuration .....	198
Remote Monitoring configuration .....	199
RMON history configuration.....	199
RMON event configuration .....	200
RMON alarm configuration.....	201
Port mirroring .....	202
Port-based port mirroring .....	203
Uplink Failure Detection configuration.....	204
Failure Detection Pair configuration .....	204
Link to Monitor configuration .....	205
Link to Disable configuration.....	206
Dump .....	207
Saving the active switch configuration .....	207
Restoring the active switch configuration .....	207
<b>Operations Menu .....</b>	<b>208</b>
Introduction .....	208
Menu information .....	208
Operations-level port options .....	208
Operations-level port 802.1X options .....	209
Operations-level VRRP options .....	210
<b>Boot Options Menu .....</b>	<b>211</b>
Introduction .....	211
Menu information .....	211
Updating the switch software image.....	211
Downloading new software to the switch .....	211
Selecting a software image to run .....	213
Uploading a software image from the switch .....	213
Selecting a configuration block.....	214
Resetting the switch .....	214
Accessing the ISCLI .....	215
<b>Maintenance Menu .....</b>	<b>216</b>

Introduction .....	216
Menu information .....	216
System maintenance options .....	217
Forwarding Database options .....	218
Debugging options .....	218
ARP cache options .....	219
IP Route Manipulation options .....	220
IGMP Multicast Group options .....	220
IGMP Snooping options .....	221
IGMP Mrouter options .....	221
Uuencode flash dump .....	222
FTP/TFTP system dump put .....	222
Clearing dump information .....	222
Panic command .....	223
Unscheduled system dumps .....	223
Index .....	224

---

# Command line interface

## Introduction

The HP 10Gb Ethernet BL-c Switch is ready to perform basic switching functions right out of the box. Some of the more advanced features, however, require some administrative configuration before they can be used effectively. This guide provides a command reference for the HP 10Gb Ethernet BL-c Switch.

The extensive switching software included in the switch provides a variety of options for accessing and configuring the switch:

- Built-in, text-based command line interfaces (AOS CLI and ISCLI) for access via a local terminal or remote Telnet/Secure Shell (SSH) session
- Simple Network Management Protocol (SNMP) support for access through network management software such as HP Systems Insight Manager
- A browser-based management interface for interactive network access through the Web browser

The command line interface provides a direct method for collecting switch information and performing switch configuration. Using a basic terminal, you can view information and statistics about the switch, and perform any necessary configuration.

This chapter explains how to access the AOS CLI to the switch.

## Additional references

Additional information about installing and configuring the switch is available in the following guides:

- *HP 10Gb Ethernet BL-c Switch User Guide*
- *HP 10Gb Ethernet BL-c Switch BladeSystem ISCLI Reference*
- *HP 10Gb Ethernet BL-c Switch Application Guide*
- *HP 10Gb Ethernet BL-c Switch Browser-based Interface Reference*
- *HP 10Gb Ethernet BL-c Switch Quick Setup Instructions*

## Connecting to the switch

You can access the command line interface in one of the following ways:

- Using a console connection via the console port
- Using a Telnet connection over the network
- Using a Secure Shell (SSH) connection to securely log in over a network



## Establishing a console connection

To establish a console connection with the switch, you need:

- A null modem cable with a female DB-9 connector (See the *HP 10Gb Ethernet BL-c Switch User Guide* for more information.)
- An ASCII terminal or a computer running terminal emulation software set to the parameters shown in the table below

**Table 1** Console configuration parameters

Parameter	Value
Baud Rate	9600
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None

To establish a console connection with the switch:

1. Connect the terminal to the console port using the null modem cable.
2. Power on the terminal.
3. Press the **Enter** key a few times on the terminal to establish the connection.
4. You will be required to enter a password for access to the switch. (For more information, see the “Setting passwords” section in the “First-time configuration” chapter.)

## Setting an IP address

To access the switch via a Telnet or an SSH connection, you need to have an Internet Protocol (IP) address set for the switch. The switch can get its IP address in one of the following ways:

- Management port access:
  - Using a Dynamic Host Control Protocol (DHCP) server—When the `/cfg/sys/dhcp` command is enabled, the management interface (interface 250) requests its IP address from a DHCP server. The default value for the `/cfg/sys/dhcp` command is enabled.
  - Configuring manually—If the network does not support DHCP, you must configure the management interface (interface 250) with an IP address. If you want to access the switch from a remote network, you also must configure the management gateway (gateway 254).
- Uplink port access:
  - Using a Bootstrap Protocol (BOOTP) server—By default, the management interface is set up to request its IP address from a BOOTP server. If you have a BOOTP server on the network, add the Media Access Control (MAC) address of the switch to the BOOTP configuration file located on the BOOTP server. The MAC address can be found in the System Information menu. (See the “System information” section in the “Information Menu” chapter.) If you are using a DHCP server that also does BOOTP, you do not have to configure the MAC address.
  - Configuring manually—If the network does not support BOOTP, you must configure the management port with an IP address.

## Establishing a Telnet connection

A Telnet connection offers the convenience of accessing the switch from any workstation connected to the network. Telnet provides the same options for user, operator, and administrator access as those available through the console port. By default, Telnet is enabled on the switch. The switch supports four concurrent Telnet connections.

Once the IP parameters are configured, you can access the CLI using a Telnet connection. To establish a Telnet connection with the switch, run the Telnet program on the workstation and enter the `telnet` command, followed by the switch IP address:

```
telnet <10GbE switch IP address>
```

You will then be prompted to enter a password. The password entered determines the access level: administrator, operator, or user. See the “Accessing the switch” section later in this chapter for description of default passwords.

## Establishing an SSH connection

Although a remote network administrator can manage the configuration of a switch via Telnet, this method does not provide a secure connection. The Secure Shell (SSH) protocol enables you to securely log into the switch over the network.

As a secure alternative to using Telnet to manage switch configuration, SSH ensures that all data sent over the network is encrypted and secure. In order to use SSH, you must first configure it on the switch. See the “Secure Shell Server configuration” section in the “Configuration Menu” chapter for information on how to configure SSH.

The switch can perform only one session of key/cipher generation at a time. Therefore, an SSH/Secure Copy (SCP) client will not be able to log in if the switch is performing key generation at that time or if another client has just logged in before this client. Similarly, the system will fail to perform the key generation if an SSH/SCP client is logging in at that time.

The supported SSH encryption and authentication methods are listed below.

- Server Host Authentication—Client RSA authenticates the switch in the beginning of every connection
- Key Exchange—RSA
- Encryption:
  - AES256-CBC
  - AES192-CBC
  - AES128-CBC
  - 3DES-CBC
  - 3DES
  - ARCFOUR
- User Authentication—Local password authentication; Remote Authentication Dial-in User Service (RADIUS)

The following SSH clients are supported:

- SSH 3.0.1 for Linux (freeware)
- SecureCRT® 4.1.8 (VanDyke Technologies, Inc.)
- OpenSSH\_3.9 for Linux (FC 3)
- FedoraCore 3 for SCP commands
- PuTTY Release 0.58 (Simon Tatham) for Windows

---

**NOTE:** The switch implementation of SSH is based on versions 1.5 and 2.0, and supports SSH clients from version 1.0 through version 2.0. SSH clients of other versions are not supported. You may configure the client software to use protocol SSH version 1 or version 2.

---

By default, SSH service is not enabled on the switch. Once the IP parameters are configured, you can access the command line interface to enable SSH.

To establish an SSH connection with the switch, run the SSH program on the workstation by issuing the `ssh` command, followed by the user account name and the switch IP address:

```
>> # ssh <user>@<10Gb switch IP address>
```

You will then be prompted to enter your password.

---

**NOTE:** The first time you run SSH from the workstation, a warning message might appear. At the prompt, enter `yes` to continue.

---

## Accessing the switch

To enable better switch management and user accountability, the switch provides different levels or classes of user access. Levels of access to the CLI and Web management functions and screens increase as needed to perform various switch management tasks. The three levels of access are:

- **User**—User interaction with the switch is completely passive; nothing can be changed on the switch. Users may display information that has no security or privacy implications, such as switch statistics and current operational state information.
- **Operator**—Operators can only effect temporary changes on the switch. These changes will be lost when the switch is rebooted/reset. Operators have access to the switch management features used for daily switch operations. Because any changes an operator makes are undone by a reset of the switch, operators cannot severely impact switch operation, but do have access to the Maintenance menu.
- **Administrator**—Only administrators can make permanent changes to the switch configuration, changes that are persistent across a reboot/reset of the switch. Administrators can access switch functions to configure and troubleshoot problems on the switch. Because administrators can also make temporary (operator-level) changes as well, they must be aware of the interactions between temporary and permanent changes.

Access to switch functions is controlled through the use of unique usernames and passwords. Once you are connected to the switch via the local console, Telnet, or SSH, you are prompted to enter a password. The password entered determines the access level. The default user names/password for each access level is listed in the following table.

---

**NOTE:** It is recommended that you change default switch passwords after initial configuration and as regularly as required under your network security policies. For more information, see the “Setting passwords” section in the “First-time configuration” chapter.

---

**Table 2** User access levels

User account	Description and tasks performed
User	The user has no direct responsibility for switch management. He or she can view all switch status information and statistics, but cannot make any configuration changes to the switch. The user account is enabled by default, and the default password is <code>user</code> .
Oper	The operator manages all functions of the switch. The operator can reset ports or the entire switch. By default, the operator account is disabled and has no password.
Admin	The super user administrator has complete access to all menus, information, and configuration commands on the switch, including the ability to change both the user and administrator passwords. The admin account is enabled by default, and the default password is <code>admin</code> .

**NOTE:** With the exception of the `admin` user, setting the password to an empty value can disable access to each user level.

Once you enter the administrator password and it is verified, you are given complete access to the switch.

After logging in, the Main Menu of the CLI is displayed. See the “Menu basics” chapter for a summary of the Main Menu options.

```
[Main Menu]
  info      - Information Menu
  stats     - Statistics Menu
  cfg       - Configuration Menu
  oper      - Operations Command Menu
  boot      - Boot Options Menu
  maint     - Maintenance Menu
  diff      - Show pending config changes [global command]
  apply     - Apply pending config changes [global command]
  save      - Save updated config to FLASH [global command]
  revert    - Revert pending or applied changes [global command]
  exit      - Exit [global command, always available]

>> Main#
```

## Idle timeout

By default, the switch will disconnect the console, Telnet, or SSH session after five minutes of inactivity. This function is controlled by the idle timeout parameter, which can be set from 1 to 60 minutes. For information on changing this parameter, see the “System configuration” section in the “Configuration Menu” chapter.

# Typographical conventions

The following table describes the typographic styles used in this guide:

**Table 3** Typographical conventions

Typeface or symbol	Meaning	Example
AaBbCc123	This type depicts onscreen computer output and prompts.	Main#
AaBbCc123	This type displays in command examples and shows text that must be typed in exactly as shown.	Main# sys
<AaBbCc123>	<p>This italicized type displays in command examples as a parameter placeholder. Replace the indicated text with the appropriate real name or value when using the command. Do not type the brackets.</p> <p>This also shows guide titles, special terms, or words to be emphasized.</p>	<p>To establish a Telnet session, enter:</p> <pre>host# telnet &lt;IP address&gt;</pre> <p>Read the user guide thoroughly.</p>
[ ]	Command items shown inside brackets are optional and can be used or excluded as the situation demands. Do not type the brackets.	host# ls [-a]

---

# Menu basics

## Introduction

The AOS CLI is used for viewing switch information and statistics. In addition, the administrator can use the CLI for performing all levels of switch configuration.

To make the CLI easy to use, the various commands have been logically grouped into a series of menus and submenus. Each menu displays a list of commands and/or submenus that are available, along with a summary of what each command will do. Below each menu is a prompt where you can enter any command appropriate to the current menu.

This chapter describes the Main Menu commands, and provides a list of commands and shortcuts that commonly are available from all the menus within the CLI.

## Main Menu

The Main Menu displays after a successful connection and login. The following table shows the Main Menu for the administrator login. Some features are not available under the user login.

[Main Menu]	
info	- Information Menu
stats	- Statistics Menu
cfg	- Configuration Menu
oper	- Operations Command Menu
boot	- Boot Options Menu
maint	- Maintenance Menu
diff	- Show pending config changes [global command]
apply	- Apply pending config changes [global command]
save	- Save updated config to FLASH [global command]
revert	- Revert pending or applied changes [global command]
exit	- Exit [global command, always available]

## Menu summary

The Main Menu displays the following submenus:

- **Information Menu**

The Information Menu provides submenus for displaying information about the current status of the switch: from basic system settings to VLANs, and more.

- **Statistics Menu**

This menu provides submenus for displaying switch performance statistics. Included are port, IP, ICMP, TCP, UDP, SNMP, routing, ARP, and DNS.

- **Configuration Menu**

This menu is available only from an administrator login. It includes submenus for configuring every aspect of the switch. Changes to configuration are not active until explicitly applied. Changes can be saved to non-volatile memory (NVRAM).

- **Operations Command Menu**

Operations-level commands are used for making immediate and temporary changes to switch configuration. This menu is used for bringing ports temporarily in and out of service. This menu is available only from an administrator and operator login.

- **Boot Options Menu**

The Boot Options Menu is available only from an administrator login. This menu is used for upgrading switch software, selecting configuration blocks, and for resetting the switch when necessary. This menu is also used to set the switch back to factory settings.

- **Maintenance Menu**

This menu is used for debugging purposes, enabling you to generate a technical support dump of the critical state information in the switch, and to clear entries in the Forwarding Database and the Address Resolution Protocol (ARP) and routing tables. This menu is available only from an administrator and operator login.

## Global commands

Some basic commands are recognized throughout the menu hierarchy. These commands are useful for obtaining online Help, navigating through menus, and for applying and saving configuration changes.

For help on a specific command, enter `help`. The following screen displays:

```
Global Commands: [can be issued from any menu]
help              up              print              pwd
lines            verbose         exit              quit
diff             apply           save              revert
ping             traceroute  telnet           history
pushd            popd              who
```

The following are used to navigate the menu structure:

- . Print current menu
- .. Move up one menu level
- / Top menu if first, or command separator
- ! Execute command from history

The following table describes the global commands.

**Table 4** Global commands

Command	Action
? command or help	Provides usage information about a specific command on the current menu. When used without the command parameter, a summary of the global commands is displayed.
. or print	Displays the current menu.
.. or up	Moves up one level in the menu structure.
/	If placed at the beginning of a command, displays the Main Menu. Otherwise, this is used to separate multiple commands placed on the same line.
lines	Sets the number of lines (n) that display on the screen at one time. The default is 24 lines. When used without a value, the current setting is displayed.
diff	Shows any pending configuration changes that have not been applied. <code>diff flash</code> displays all pending configuration changes that have been applied but not saved to flash memory (NVRAM), as well as those that have not been applied.
apply	Applies pending configuration changes.

**Table 4** Global commands

Command	Action
save	Saves the active configuration to backup, and saves the current configuration as active. save n saves the current configuration as active, without saving the active configuration to backup.
revert	Removes changes that have been made, but not applied. revert apply removes all changes that have not been saved.
Exit or quit	Exits from the command line interface and logs out.
ping	Verifies station-to-station connectivity across the network. The format is: ping <host name> <IP address> [attempts (1-32)> [msec delay]] [-m -mgt -d -data] <ul style="list-style-type: none"> <li>• <i>IP address</i> is the hostname or IP address of the device.</li> <li>• <i>number of tries</i> (optional) is the number of attempts (1-32).</li> <li>• <i>msec delay</i> (optional) is the number of milliseconds between attempts.</li> <li>• By default, the <b>-m</b> or <b>-mgt</b> option for the management port is used. To use data ports, specify the <b>-d</b> or <b>-data</b> option.</li> </ul>
tracert	Identifies the route used for station-to-station connectivity across the network. The format is: tracert <host name> <IP address> [<max-hops> [ msec delay ]] <ul style="list-style-type: none"> <li>• <i>IP address</i> is the hostname or IP address of the target station.</li> <li>• <i>max-hops</i> (optional) is the maximum distance to trace (1-32 devices).</li> <li>• <i>msec delay</i> (optional) is the number of milliseconds to wait for the response.</li> </ul>
pwd	Displays the command path used to reach the current menu.
verbose n	Sets the level of information displayed on the screen: <ul style="list-style-type: none"> <li>• 0 = Quiet: Nothing displays except errors, not even prompts.</li> <li>• 1 = Normal: Prompts and requested output are shown, but no menus.</li> <li>• 2 = Verbose: Everything is shown. This is the default.</li> <li>• When used without a value, the current setting is displayed.</li> </ul>
telnet	This command is used to Telnet out of the switch. The format is: telnet <hostname>   <IP address> [port] [-m -mgt -d -data] <p>By default, the <b>-m</b> or <b>-mgt</b> option for the management port is used. To use data ports, specify the <b>-d</b> or <b>-data</b> option.</p>
history	Displays the history of the last ten commands.
pushd	Remembers the current location in the directory of menu commands.
popd	Returns to the last pushd location.
who	Displays users who are logged in.



# Command line history and editing

Using the command line interface, you can retrieve and modify previously entered commands with just a few keystrokes. The following options are available globally at the command line:

**Table 5** Command line history and editing options

Option	Description
history	Displays a numbered list of the last ten previously entered commands.
!!	Repeats the last entered command.
!n	Repeats the nth command shown on the history list.
<Ctrl-p> or <b>Up arrow</b> key	Recalls the previous command from the history list. This can be used multiple times to work backward through the last ten commands. The recalled command can be entered as is, or edited using the options below.
<Ctrl-n> or <b>Down arrow</b> key	Recalls the next command from the history list. This can be used multiple times to work forward through the last ten commands. The recalled command can be entered as is, or edited using the options below.
<Ctrl-a>	Moves the cursor to the beginning of the command line.
<Ctrl-e>	Moves cursor to the end of the command line.
<Ctrl-b> or <b>Left arrow</b> key	Moves the cursor back one position to the left.
<Ctrl-f> or <b>Right arrow</b> key	Moves the cursor forward one position to the right.
<Backspace> or <b>Delete</b> key	Erases one character to the left of the cursor position.
<Ctrl-d>	Deletes one character at the cursor position.
<Ctrl-k>	Erases all characters from the cursor position to the end of the command line.
<Ctrl-l>	Redisplays the current line.
<Ctrl-u>	Clears the entire line.
Other keys	Inserts new characters at the cursor position.
.	Prints the current level menu list.
..	Moves to the previous directory level.

# Command line interface shortcuts

The following shortcuts allow you to enter commands quickly and easily.

## Command stacking

As a shortcut, you can type multiple commands on a single line, separated by forward slashes (/). You can connect as many commands as required to access the menu option that you want.

For example, the keyboard shortcut to access the Simple Network Management Protocol (SNMP) Configuration Menu from the Main# prompt is:

```
Main# cfg/sys/ssnmp/name
```

## Command abbreviation

Most commands can be abbreviated by entering the first characters that distinguish the command from the others in the same menu or submenu.

For example, the command shown above could also be entered as:

```
Main# c/sys/ssn/n
```

## Tab completion

By entering the first letter of a command at any menu prompt and pressing the Tab key, the CLI will display all commands or options in that menu that begin with that letter. Entering additional letters will further refine the list of commands or options displayed.

If only one command fits the input text when the Tab key is pressed, that command will be supplied on the command line, waiting to be entered. If the Tab key is pressed without any input on the command line, the currently active menu displays.

---

# First-time configuration

## Introduction

This chapter describes how to perform first-time configuration and how to change system passwords.

To begin first-time configuration of the switch, perform the following steps.

1. Connect to the switch console. After connecting, the login prompt displays.

```
HP 10Gb Ethernet BL-c Switch
Copyright (C) 2006 Hewlett-Packard Development Company, L.P.
Password:
```

2. Enter admin as the default administrator password.

The system displays the Main Menu with administrator privileges.

```
[Main Menu]
info      - Information Menu
stats     - Statistics Menu
cfg       - Configuration Menu
oper      - Operations Command Menu
boot      - Boot Options Menu
maint     - Maintenance Menu
diff      - Show pending config changes [global command]
apply     - Apply pending config changes [global command]
save      - Save updated config to FLASH [global command]
revert    - Revert pending or applied changes [global command]
exit      - Exit [global command, always available]

>> Main#
```

3. From the Main Menu, enter the following command to access the Configuration Menu:

```
Main# /cfg
```

The Configuration Menu is displayed.

```
[Configuration Menu]
sys       - System-wide Parameter Menu
port      - Port Menu
l2        - Layer 2 Menu
l3        - Layer 3 Menu
qos       - QOS Menu
acl       - Access Control List Menu
rmon      - RMON Menu
pmirr     - Port Mirroring Menu
ufd       - Uplink Failure Detection Menu
dump      - Dump current configuration to script file
ptcfg     - Backup current configuration to FTP/TFTP server
gtcfg     - Restore current configuration from FTP/TFTP server
cur       - Display current configuration
```

# Configuring Simple Network Management Protocol support

**NOTE:** SNMP support is enabled by default.

1. Use the following command to enable SNMP:

```
>> # /cfg/sys/access/snmp disable|read only|read/write
```

2. Set SNMP read or write community string. By default, they are public and private respectively:

```
>> # /cfg/sys/ssnmp/rcomm|wcomm
```

3. When prompted, enter the proper community string.

4. Apply and save configuration if you are not configuring the switch with Telnet support. Otherwise apply and save after the performing the “Optional Setup for Telnet Support” steps.

```
>> System# apply
>> System# save
```

## Setting passwords

HP recommends that you change all passwords after initial configuration and as regularly as required under the network security policies. See the “Accessing the switch” section in the “Command line interface” chapter for a description of the user access levels.

To change the user, operator, or administrator password, you must log in using the administrator password. Passwords cannot be modified from the user or operator command mode.

**NOTE:** If you forget your administrator password, call HP technical support for help using the password fix-up mode.

## Changing the default administrator password

The administrator has complete access to all menus, information, and configuration commands, including the ability to change the user, operator, and administrator passwords.

The default password for the administrator account is admin. To change the default password:

1. Connect to the switch and log in using the admin password.
2. From the Main Menu, use the following command to access the Configuration Menu:

```
Main# /cfg
```

The Configuration Menu is displayed.

```
[Configuration Menu]
sys      - System-wide Parameter Menu
port     - Port Menu
l2       - Layer 2 Menu
l3       - Layer 3 Menu
qos      - QOS Menu
acl      - Access Control List Menu
rmon     - RMON Menu
pmirr    - Port Mirroring Menu
ufd      - Uplink Failure Detection Menu
dump     - Dump current configuration to script file
ptcfg    - Backup current configuration to FTP/TFTP server
gtcfg    - Restore current configuration from FTP/TFTP server
cur      - Display current configuration
```

3. From the Configuration Menu, use the following command to select the System Menu:

```
>> Configuration# sys
```

The System Menu is displayed.

```
[System Menu]
  syslog      - Syslog Menu
  sshd        - SSH Server Menu
  radius      - RADIUS Authentication Menu
  tacacs+     - TACACS+ Authentication Menu
  ntp         - NTP Server Menu
  ssnmp       - System SNMP Menu
  access      - System Access Menu
  date        - Set system date
  time        - Set system time
  timezone    - Set system timezone (daylight savings)
  olddst      - Set system DST for US
  dlight      - Set system daylight savings
  idle        - Set timeout for idle CLI sessions
  notice      - Set login notice
  bannr       - Set login banner
  hprompt     - Enable/disable display hostname (sysName) in CLI prompt
  bootp       - Enable/disable use of BOOTP
  dhcp        - Enable/disable use of DHCP on Mgmt interface
  reminders   - Enable/disable Reminders
  cur         - Display current system-wide parameters
```

4. Enter the following command to set the administrator password:

```
System# access/user/admpw
```

5. Enter the current administrator password at the prompt:

```
Changing ADMINISTRATOR password; validation required...
Enter current administrator password:
```

---

**NOTE:** If you forget your administrator password, call your technical support representative for help using the password fix-up mode.

---

6. Enter the new administrator password at the prompt:

```
Enter new administrator password:
```

7. Enter the new administrator password, again, at the prompt:

```
Re-enter new administrator password:
```

8. Apply and save the change by entering the following commands:

```
System# apply
System# save
```

## Changing the default user password

The user login has limited control of the switch. Through a user account, you can view switch information and statistics, but you cannot make configuration changes.

The default password for the user account is user. This password cannot be changed from the user account. Only the administrator has the ability to change passwords, as shown in the following procedure.

1. Connect to the switch and log in using the `admin` password.
2. From the Main Menu, use the following command to access the Configuration Menu:

```
Main# cfg
```

3. From the Configuration Menu, use the following command to select the System Menu:

```
>> Configuration# sys
```

4. Enter the following command to set the user password:

```
System# access/user/usrpw
```

5. Enter the current administrator password at the prompt.

Only the administrator can change the user password. Entering the administrator password confirms your authority.

```
Changing USER password; validation required...
Enter current administrator password:
```

6. Enter the new user password at the prompt:

```
Enter new user password:
```

7. Enter the new user password, again, at the prompt:

```
Re-enter new user password:
```

8. Apply and save the changes:

```
System# apply
System# save
```

## Changing the default operator password

The operator manages all functions of the switch. The operator can reset ports or the entire switch. Operators can only effect temporary changes on the switch. These changes will be lost when the switch is rebooted/reset. Operators have access to the switch management features used for daily switch operations. Because any changes an operator makes are undone by a reset of the switch, operators cannot severely impact switch operation.

By default, the operator account is disabled and has no password. This password cannot be changed from the operator account. Only the administrator has the ability to change passwords, as shown in the following procedure.

1. Connect to the switch and log in using the `admin` password.
2. From the Main Menu, use the following command to access the Configuration Menu:

```
Main# cfg
```

3. From the Configuration Menu, use the following command to select the System Menu:

```
>> Configuration# sys
```

4. Enter the following command to set the operator password:

```
System# access/user/opw
```

5. Enter the current administrator password at the prompt.

Only the administrator can change the user password. Entering the administrator password confirms your authority.

```
Changing OPERATOR password; validation required...  
Enter current administrator password:
```

6. Enter the new operator password at the prompt:

```
Enter new operator password:
```

7. Enter the new operator password, again, at the prompt:

```
Re-enter new operator password:
```

8. Apply and save the changes:

```
System# apply  
System# save
```

# Information Menu

## Introduction

You can view configuration information for the switch in the user, operator, and administrator command modes. This chapter discusses how to use the CLI to display switch information.

## Menu overview

**Command:** `/info`

```
[Information Menu]
  sys      - System Information Menu
  l2       - Layer 2 Information Menu
  l3       - Layer 3 Information Menu
  qos      - QoS Menu
  acl      - Show ACL information
  rmon     - Show RMON information
  link     - Show link status
  port     - Show port information
  transcvr - Show Port Transceiver status
  ufd      - Show Uplink Failure Detection information
  sfd      - Show Server Link Failure Detection information
  dump     - Dump all information
```

The following table describes the Information Menu options.

**Table 6** Information Menu options

Command	Usage
sys	Displays system information.
l2	Displays the Layer 2 Information Menu.
l3	Displays the Layer 3 Information Menu.
qos	Displays the Quality of Service (QoS) Information Menu.
acl	Displays the Access Control List Information Menu.
rmon	Displays the Remote Monitoring Information Menu.
link	Displays configuration information about each port, including: <ul style="list-style-type: none"><li>• Port number</li><li>• Port speed</li><li>• Duplex mode (half, full, or any)</li><li>• Flow control for transmit and receive (no, yes, or any)</li><li>• Link status (up or down)</li></ul>



**Table 6** Information Menu options

Command	Usage
port	Displays port status information, including: <ul style="list-style-type: none"> <li>• Port number</li> <li>• Whether the port uses VLAN tagging or not</li> <li>• Port VLAN ID (PVID)</li> <li>• Port name</li> <li>• VLAN membership</li> </ul>
transcvr	Displays the status of the Small Form Pluggable (SFP) module on each Fiber External Port.
ufd	Displays Uplink Failure Detection information.
sfd	Displays Server Link Failure Detection information.
dump	Dumps all switch information available from the Information Menu (10K or more, depending on your configuration). If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.

## System Information Menu

**Command:** /info/sys

```
[System Menu]
snmpv3  - SNMPv3 Information Menu
general - Show general system information
log     - Show last 100 syslog messages
user    - Show current user status
dump    - Dump all system information
```

The following table describes the System Information Menu options.

**Table 7** System Information Menu options

Command	Usage
snmpv3	Displays the SNMP v3 Menu.
general	Displays system information, including: <ul style="list-style-type: none"> <li>• System date and time</li> <li>• Switch model name and number</li> <li>• Switch name and location</li> <li>• Time of last boot</li> <li>• MAC address of the switch management processor</li> <li>• IP address of IP interface #1</li> <li>• Hardware version and part number</li> <li>• Software image file and version number</li> <li>• Configuration name</li> <li>• Log-in banner, if one is configured</li> </ul>
log	Displays 100 most recent syslog messages.

**Table 7** System Information Menu options

Command	Usage
user	Displays the User Access Information Menu.
dump	Dumps all switch information available from the Information Menu (10K or more, depending on your configuration).

## SNMPv3 Information Menu

**Command:** /info/sys/snmpv3

```
[SNMPv3 Information Menu]
  usm      - Show usmUser table information
  view     - Show vacmViewTreeFamily table information
  access   - Show vacmAccess table information
  group    - Show vacmSecurityToGroup table information
  comm     - Show community table information
  taddr    - Show targetAddr table information
  tparam   - Show targetParams table information
  notify   - Show notify table information
  dump     - Show all SNMPv3 information
```

SNMP version 3 (SNMPv3) is an extensible SNMP Framework that supplements the SNMPv2 Framework by supporting the following:

- a new SNMP message format
- security for messages
- access control
- remote configuration of SNMP parameters

For more details on the SNMPv3 architecture, see RFC2271 to RFC2276.

The following table describes the SNMPv3 Information Menu options.

**Table 8** SNMPv3 Information Menu options

Command	Usage
usm	Displays User Security Model (USM) table information.
view	Displays information about view name, subtrees, mask and type of view.
access	Displays View-based Access Control information.
group	Displays information about the group that includes the security model, user name, and group name.
comm	Displays information about the community table.
taddr	Displays the Target Address table.
tparam	Displays the Target parameters table.
notify	Displays the Notify table.
dump	Displays all the SNMPv3 information.

## SNMPv3 USM User Table information

**Command:** /info/sys/snmpv3/usm

```
usmUser Table:
User Name                                Protocol
-----
adminmd5                                HMAC_MD5, DES PRIVACY
adminsha                                HMAC_SHA, DES PRIVACY
v1v2only                                NO AUTH, NO PRIVACY
```

The User-based Security Model (USM) in SNMPv3 provides security services such as authentication and privacy of messages. This security model makes use of a defined set of user identities displayed in the USM user table. The USM user table contains information like:

- the user name
- a security name in the form of a string whose format is independent of the Security Model
- an authentication protocol, which is an indication that the messages sent on behalf of the user can be authenticated
- the privacy protocol.

The following table describes the SNMPv3 User Table information.

**Table 9** User Table parameters

Field	Description
User Name	This is a string that represents the name of the user that you can use to access the switch.
Protocol	This indicates whether messages sent on behalf of this user are protected from disclosure using a privacy protocol. Switch software supports DES algorithm for privacy. The software also supports two authentication algorithms: MD5 and HMAC-SHA.

## SNMPv3 View Table information

**Command:** /info/sys/snmpv3/view

View Name	Subtree	Mask	Type
-----	-----	-----	-----
iso	1		included
v1v2only	1		included
v1v2only	1.3.6.1.6.3.15		excluded
v1v2only	1.3.6.1.6.3.16		excluded
v1v2only	1.3.6.1.6.3.18		excluded

The user can control and restrict the access allowed to a group to only a subset of the management information in the management domain that the group can access within each context by specifying the group's rights in terms of a particular MIB view for security reasons.

The following table describes the SNMPv3 View Table information.

**Table 10** View Table parameters

Field	Description
View Name	Displays the name of the view.
Subtree	Displays the MIB subtree as an OID string. A view subtree is the set of all MIB object instances which have a common Object Identifier prefix to their names.
Mask	Displays the bit mask.
Type	Displays whether a family of view subtrees is included or excluded from the MIB view.

## SNMPv3 Access Table information

**Command:** /info/sys/snmpv3/access

Group Name	Model	Level	ReadV	WriteV	NotifyV
-----	-----	-----	-----	-----	-----
v1v2grp	snmpv1	noAuthNoPriv	iso	iso	v1v2only
admingrp	usm	authPriv	iso	iso	iso

The access control sub system provides authorization services.

The vacmAccessTable maps a group name, security information, a context, and a message type, which could be the read or write type of operation or notification into a MIB view.

The View-based Access Control Model defines a set of services that an application can use for checking access rights of a group. This group's access rights are determined by a read-view, a write-view, and a notify-view. The read-view represents the set of object instances authorized for the group while reading the objects. The write-view represents the set of object instances authorized for the group when writing objects. The notify-view represents the set of object instances authorized for the group when sending a notification.

The following table describes the SNMPv3 Access Table information.

**Table 11** Access Table parameters

Field	Description
Group Name	Displays the name of group.
Prefix	Displays the prefix that is configured to match the values.
Model	Displays the security model used, for example, SNMPv1, or SNMPv2 or USM.
Level	Displays the minimum level of security required to gain rights of access. For example, noAuthNoPriv, authNoPriv, or auth-Priv.
ReadV	Displays the MIB view to which this entry authorizes the read access.
WriteV	Displays the MIB view to which this entry authorizes the write access.
NotifyV	Displays the Notify view to which this entry authorizes the notify access.

## SNMPv3 Group Table information

**Command:** `/info/sys/snmpv3/group`

Sec Model	User Name	Group Name
-----	-----	-----
snmpv1	v1v2only	v1v2grp
usm	adminmd5	admingrp
usm	adminsha	admingrp

A group is a combination of security model and security name that defines the access rights assigned to all the security names belonging to that group. The group is identified by a group name.

The following table describes the SNMPv3 Group Table information.

**Table 12** Group Table parameters

Field	Description
Sec Model	Displays the security model used, which is any one of: USM, SNMPv1, SNMPv2, and SNMPv3.
User Name	Displays the name for the group.
Group Name	Displays the access name of the group.

## SNMPv3 Community Table information

**Command:** `/info/sys/snmpv3/comm`

Index	Name	User Name	Tag
-----	-----	-----	-----
trap1	public	v1v2only	v1v2trap

This command displays the community table information stored in the SNMP engine.

The following table describes the SNMPv3 Community Table information.

**Table 13** Community Table parameters

Field	Description
Index	Displays the unique index value of a row in this table.
Name	Displays the community string, which represents the configuration.
User Name	Displays the User Security Model (USM) user name.
Tag	Displays the community tag. This tag specifies a set of transport endpoints from which a command responder application accepts management requests and to which a command responder application sends an SNMP trap.

## SNMPv3 Target Address Table information

**Command:** /info/sys/snmpv3/taddr

Name	Transport Addr	Port	Taglist	Params
-----	-----	----	-----	-----
trap1	47.81.25.66	162	v1v2trap	v1v2param

This command displays the SNMPv3 target address table information, which is stored in the SNMP engine.

The following table describes the SNMPv3 Target Address Table information.

**Table 14** Target Address Table parameters

Field	Description
Name	Displays the locally arbitrary, but unique identifier associated with this snmpTargetAddrEntry.
Transport Addr	Displays the transport addresses.
Port	Displays the SNMP UDP port number.
Taglist	This column contains a list of tag values which are used to select target addresses for a particular SNMP message.
Params	The value of this object identifies an entry in the snmpTargetParamsTable. The identified entry contains SNMP parameters to be used when generating messages to be sent to this transport address.

## SNMPv3 Target Parameters Table information

**Command:** /info/sys/snmpv3/tparam

Name	MP Model	User Name	Sec Model	Sec Level
-----	-----	-----	-----	-----
v1v2param	snmpv2c	v1v2only	snmpv1	noAuthNoPriv

The following table describes the SNMPv3 Target Parameters Table information.

**Table 15** Target Parameters Table

Field	Description
Name	Displays the locally arbitrary, but unique identifier associated with this snmpTargeParamsEntry.
MP Model	Displays the Message Processing Model used when generating SNMP messages using this entry.
User Name	Displays the securityName, which identifies the entry on whose behalf SNMP messages will be generated using this entry.
Sec Model	Displays the security model used when generating SNMP messages using this entry. The system may choose to return an inconsistentValue error if an attempt is made to set this variable to a value for a security model which the system does not support.
Sec Level	Displays the level of security used when generating SNMP messages using this entry.

## SNMPv3 Notify Table information

**Command:** `/info/sys/snmpv3/notify`

Name	Tag
-----	-----
v1v2trap	v1v2trap

The following table describes the SNMPv3 Notify Table information.

**Table 16** SNMPv3 Notify Table

Field	Description
Name	The locally arbitrary, but unique identifier associated with this snmpNotifyEntry.
Tag	This represents a single tag value which is used to select entries in the snmpTargetAddrTable. Any entry in the snmpTargetAddrTable that contains a tag value equal to the value of this entry is selected. If this entry contains a value of zero length, no entries are selected.

# SNMPv3 dump

**Command:** /info/sys/snmpv3/dump

```
Engine ID = 80:00:07:50:03:00:0F:6A:F8:EF:00
usmUser Table:
User Name                                Protocol
-----
admin                                    NO AUTH, NO PRIVACY
adminmd5                                HMAC_MD5, DES PRIVACY
adminsha                                HMAC_SHA, DES PRIVACY
v1v2only                                NO AUTH, NO PRIVACY

vacmAccess Table:
Group Name Prefix Model Level Match ReadV WriteV NotifyV
-----
admin                usm    noAuthNoPriv exact  org    org    org
v1v2grp              snmpv1 noAuthNoPriv exact  org    org    v1v2only
admingrp             usm    authPriv    exact  org    org    org

vacmViewTreeFamily Table:
View Name Subtree Mask Type
-----
org        1.3      included
v1v2only   1.3      included
v1v2only   1.3.6.1.6.3.15 excluded
v1v2only   1.3.6.1.6.3.16 excluded
v1v2only   1.3.6.1.6.3.18 excluded

vacmSecurityToGroup Table:
Sec Model User Name Group Name
-----
snmpv1     v1v2only v1v2grp
usm         admin   admin
usm         adminsha admingrp

snmpCommunity Table:
Index Name User Name Tag
-----

snmpNotify Table:
Name Tag
-----

snmpTargetAddr Table:
Name Transport Addr Port Taglist Params
-----

snmpTargetParams Table:
Name MP Model User Name Sec Model Sec Level
-----
```



## System information

**Command:** `/info/sys/gen`

```
System Information at 6:56:22 Thu Jan 10, 2008
Time zone: America/US/Pacific

HP 10Gb Ethernet BL-c Switch
sysName:
sysLocation:
RackName: Default Rack Name
EnclosureName: Default Chassis Name
BayNumber: 1

Switch has been up for 3 days, 14 hours, 56 minutes and 22 seconds.
Last boot: 17:25:38 Mon Jan 8, 2007 (software reset)

MAC address: 00:10:00:01:00:01      IP (If 1) address: 10.14.4.16
Management Port MAC Address: 00:10:18:00:00:00
Management Port IP Address (if 250): 10.20.7.15
Revision: 0A
Switch Serial No: BLK7GEFR-3
Hardware Part No: 445680-B21      Spare Part No: 447126-001
Software Version 4.0.0 (FLASH image2), active configuration.
```

System information includes:

- System date and time
- Switch model name and number
- HP c-Class Rack name and location
- Time of last boot
- MAC address of the switch management processor
- IP address of the switch
- Software image file and version number
- Current configuration block (active, backup, or factory default)
- Login banner, if one is configured

## Show last 100 syslog messages

**Command:** /info/sys/log

Date	Time	Severity level	Message
----	----	-----	-----
Jul 8	17:25:41	NOTICE	system: link up on port 1
Jul 8	17:25:41	NOTICE	system: link up on port 8
Jul 8	17:25:41	NOTICE	system: link up on port 7
Jul 8	17:25:41	NOTICE	system: link up on port 12
Jul 8	17:25:41	NOTICE	system: link up on port 11
Jul 8	17:25:41	NOTICE	system: link up on port 14
Jul 8	17:25:41	NOTICE	system: link up on port 13
Jul 8	17:25:41	NOTICE	system: link up on port 16
Jul 8	17:25:41	NOTICE	system: link up on port 15
Jul 8	17:25:41	NOTICE	system: link up on port 17
Jul 8	17:25:41	NOTICE	system: link up on port 20
Jul 8	17:25:41	NOTICE	system: link up on port 18
Jul 8	17:25:41	NOTICE	system: link up on port 19
Jul 8	17:25:41	NOTICE	system: link up on port 21
Jul 8	17:25:42	NOTICE	system: link up on port 4
Jul 8	17:25:42	NOTICE	system: link up on port 3
Jul 8	17:25:42	NOTICE	system: link up on port 6
Jul 8	17:25:42	NOTICE	system: link up on port 5
Jul 8	17:25:42	NOTICE	system: link up on port 10
Jul 8	17:25:42	NOTICE	system: link up on port 9

Each message contains a date and time field and has a severity level associated with it. One of eight different prefixes is used to indicate the condition:

- EMERG—indicates the system is unusable
- ALERT—indicates action should be taken immediately
- CRIT—indicates critical conditions
- ERR—indicates error conditions or eroded operations
- WARNING—indicates warning conditions
- NOTICE—indicates a normal but significant condition
- INFO—indicates an information message
- DEBUG—indicates a debug-level message

## System user information

**Command:** `/info/sys/user`

Usernames:

```
user      - enabled
oper      - disabled
admin     - Always Enabled
```

Current User ID table:

```
1: name tech1   , ena, cos user   , password valid, online
2: name tech2   , ena, cos user   , password valid, offline
```

The following table describes the User Name information.

**Table 17** User Name information menu

Field	Usage
user	Displays the status of the user access level.
oper	Displays the status of the oper (operator) access level.
admin	Displays the status of the admin (administrator) access level.
Current User ID Table	Displays the status of configured user IDs. To configure new user IDs, use the <code>/cfg/sys/access/user/uid</code> command.

# Layer 2 information

**Command:** /info/l2

```
[Layer 2 Menu]
fdb      - Forwarding Database Information Menu
lacp     - Link Aggregation Control Protocol Menu
hotlink  - Show Hot Links information
8021x    - Show 802.1X information
stp      - Show STP information
cist     - Show CIST information
trunk    - Show Trunk Group information
vlan     - Show VLAN information
uplink   - Show uplink information
dump     - Dump all layer 2 information
```

The following table describes the Layer 2 Information Menu options.

**Table 18** Layer 2 Information Menu options

Command	Usage
fdb	Displays the Forwarding Database Information Menu.
lacp	Displays the Link Aggregation Control Protocol Information Menu.
hotlink	Displays the Hot Links Information Menu.
8021x	Displays the 802.1X Information Menu.
stp	<p>In addition to seeing if STP is enabled or disabled, you can view the following STP bridge information:</p> <ul style="list-style-type: none"><li>• Priority</li><li>• Hello interval</li><li>• Maximum age value</li><li>• Forwarding delay</li><li>• Aging time</li></ul> <p>You can also refer to the following port-specific STP information:</p> <ul style="list-style-type: none"><li>• Port number and priority</li><li>• Cost</li><li>• State</li></ul>
cist	<p>Displays Common internal Spanning Tree (CIST) bridge information, including the following:</p> <ul style="list-style-type: none"><li>• Priority</li><li>• Hello interval</li><li>• Maximum age value</li><li>• Forwarding delay</li></ul> <p>You can also view port-specific CIST information, including the following:</p> <ul style="list-style-type: none"><li>• Port number and priority</li><li>• Cost</li><li>• State</li></ul>
trunk	When trunk groups are configured, you can view the state of each port in the various trunk groups.

**Table 18** Layer 2 Information Menu options

Command	Usage
vlan	Displays VLAN configuration information, including: <ul style="list-style-type: none"> <li>• VLAN Number</li> <li>• VLAN Name</li> <li>• Status</li> <li>• Port membership of the VLAN</li> </ul>
uplink	Displays the status of Spanning Tree Uplink Fast.
dump	Dumps all switch information available from the Layer 2 menu (10K or more, depending on your configuration).  If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.

## FDB information menu

**Command:** /info/l2/fdb

```
[Forwarding Database Menu]
  find    - Show a single FDB entry by MAC address
  port    - Show FDB entries on a single port
  vlan    - Show FDB entries on a single VLAN
  state   - Show FDB entries by state
  dump    - Show all FDB entries
```

The forwarding database (FDB) contains information that maps the media access control (MAC) address of each known device to the switch port where the device address was learned. The FDB also shows which other ports have seen frames destined for a particular MAC address.

**NOTE:** The master forwarding database supports up to 8K MAC address entries on the management processor (MP) per switch.

**Table 19** FDB information menu

Command	Usage
find <MAC address> [<VLAN>]	Displays a single database entry by its MAC address. You are prompted to enter the MAC address of the device. Enter the MAC address using the format: xx:xx:xx:xx:xx:xx. (For example: 08:00:20:12:34:56) You can also enter the MAC address using the format: xxxxxxxxxxxx. (For example: 080020123456)
port <port number>	Displays all FDB entries for a particular port.
vlan <1-4095>	Displays all FDB entries on a single VLAN. The range is 1-4095.
state unknown ignore forward flood trunk ifmac	Displays all FDB entries that match a particular state.
dump	Displays all entries in the Forwarding Database.

## Show all FDB information

**Command:** `/info/l2/fdb/dump`

MAC address	VLAN	Port	Trnk	State
-----	----	----	----	-----
00:02:01:00:00:00	300		1	TRK
00:02:01:00:00:01	300	20		FWD
00:02:01:00:00:02	300	20		FWD
00:02:01:00:00:03	300	20		FWD
00:02:01:00:00:04	300	20		FWD
00:02:01:00:00:05	300	20		FWD
00:02:01:00:00:06	300	20		FWD
00:02:01:00:00:07	300	20		FWD
00:02:01:00:00:08	300	20		FWD
00:02:01:00:00:09	300	20		FWD
00:02:01:00:00:0a	300	20		FWD
00:02:01:00:00:0b	300	20		FWD
00:02:01:00:00:0c	300	20		FWD

An address that is in the forwarding (FWD) state indicates that the switch has learned it. When in the trunking (TRK) state, the Trnk field displays the trunk group number. If the state for the port is listed as unknown (UNK), the MAC address has not yet been learned by the switch, but has only been seen as a destination address. When an address is in the unknown state, no outbound port is indicated.

## Clearing entries from the forwarding database

To delete a static MAC address from the forwarding database (FDB), see the “Static FDB configuration” section in the “Configuration Menu” chapter. To clear the entire forwarding database (FDB), see the “Forwarding Database options” section in the “Maintenance Menu” chapter.

## Link Aggregation Control Protocol information

**Command:** `/info/l2/lacp`

```
[LACP Menu]
  aggr      - Show LACP aggregator information for the port
  port      - Show LACP port information
  dump      - Show all LACP ports information
```

The following table describes the Link Aggregation Control Protocol Menu options.

**Table 20** LACP information

Command	Usage
aggr	Displays LACP aggregator information for the port.
port	Displays LACP information for the port.
dump	Displays all LACP information parameters.

## LACP dump

**Command:** /info/l2/lacp/dump

```
>> LACP# dump
port lacp adminkey operkey selected prio attached trunk
      aggr
-----
 1  off      1         1         n    32768    --      --
 2  off      2         2         n    32768    --      --
 3  off      3         3         n    32768    --      --
 4  off      4         4         n    32768    --      --
 5  off      5         5         n    32768    --      --
 6  off      6         6         n    32768    --      --
 7  off      7         7         n    32768    --      --
 8  off      8         8         n    32768    --      --
...
```

LACP dump includes the following information for each port in the switch:

- lacp—Displays the port's LACP mode (active, passive, or off)
- adminkey—Displays the value of the port's adminkey.
- operkey—Shows the value of the port's operational key.
- selected—Indicates whether the port has been selected to be part of a Link Aggregation Group.
- prio—Shows the value of the port priority.
- attached aggr—Displays the aggregator associated with each port.
- trunk—This value represents the LACP trunk group number.

## Hot Links Trigger information

**Command:** /info/l2/hotlink/trigger

```
Hot Links Info: Trigger

Current global Hot Links setting: ON
bpdu disabled
sndfdb disabled

Current Trigger 1 setting: enabled
name "Trigger 1", preempt enabled, fdelay 1 sec

Active state: None

Master settings:
    port 20
Backup settings:
    port 21
```

Hot Links trigger information includes the following:

- Hot Links status (on or off)
- Status of BPDU flood option
- Status of FDB send option
- Status and configuration of each Hot Links trigger

## 802.1X information

**Command:** /info/l2/8021x

```
System capability : Authenticator
System status    : disabled
Protocol version : 1

Port   Auth Mode   Auth Status   Authenticator PAE State   Backend Auth State
-----
1      force-auth   unauthorized   initialize    initialize
2      force-auth   unauthorized   initialize    initialize
3      force-auth   unauthorized   initialize    initialize
4      force-auth   unauthorized   initialize    initialize
5      force-auth   unauthorized   initialize    initialize
6      force-auth   unauthorized   initialize    initialize
7      force-auth   unauthorized   initialize    initialize
8      force-auth   unauthorized   initialize    initialize
9      force-auth   unauthorized   initialize    initialize
10     force-auth   unauthorized   initialize    initialize
11     force-auth   unauthorized   initialize    initialize
12     force-auth   unauthorized   initialize    initialize
13     force-auth   unauthorized   initialize    initialize
14     force-auth   unauthorized   initialize    initialize
15     force-auth   unauthorized   initialize    initialize
16     force-auth   unauthorized   initialize    initialize
*18    force-auth   unauthorized   initialize    initialize
*19    force-auth   unauthorized   initialize    initialize
*20    force-auth   unauthorized   initialize    initialize
*21    force-auth   unauthorized   initialize    initialize
-----
* - Port down or disabled
```

The following table describes the IEEE 802.1X parameters.

**Table 21** 802.1X information

Field	Description
Port	Displays each port's name.
Auth Mode	Displays the Access Control authorization mode for the port. The Authorization mode can be one of the following: <ul style="list-style-type: none"><li>• force-unauth</li><li>• auto</li><li>• force-auth</li></ul>
Auth Status	Displays the current authorization status of the port, either authorized or unauthorized.



**Table 21** 802.1X information

Field	Description
Authenticator PAE State	Displays the Authenticator Port Access Entity State. The PAE state can be one of the following: <ul style="list-style-type: none"><li>• initialize</li><li>• disconnected</li><li>• connecting</li><li>• authenticating</li><li>• authenticated</li><li>• aborting</li><li>• held</li><li>• forceAuth</li></ul>
Backend Auth State	Displays the Backend Authorization State. The Backend Authorization state can be one of the following: <ul style="list-style-type: none"><li>• request</li><li>• response</li><li>• success</li><li>• fail</li><li>• timeout</li><li>• idle</li></ul>

# Spanning Tree information

**Command:** /info/l2/stp

```
-----
upfast disabled, update 40
BPDU Guard disabled
Pvst+ compatibility mode enabled
-----

Spanning Tree Group 1: On (STP/PVST+)
VLANs: 1

Current Root:          Path-Cost      Port   Hello MaxAge FwdDel
8000 00:02:a5:d1:0f:ed      8       20     2      20     15

Parameters:  Priority  Hello  MaxAge  FwdDel  Aging
              32768    2      20     15     300

Port  Priority  Cost  FastFwd  State          Designated Bridge  Des Port
-----
  1      0      0      n    FORWARDING *
  2      0      0      n    FORWARDING *
  3      0      0      n    FORWARDING *
```

The switch software uses the IEEE 802.1D Spanning Tree Protocol (STP). If RSTP/MSTP is turned on, see the “Rapid Spanning Tree information” section for Spanning Tree Group information. In addition to seeing if STP is enabled or disabled, you can view the following STP bridge information:

- Status of Uplink Fast (upfast)
- Current root MAC address
- Path-Cost
- Port
- Hello interval
- Maximum age value
- Forwarding delay
- Aging time

You can also refer to the following port-specific STP information:

- Port number and priority
- Cost
- State
- Port Fast Forwarding state
- Designated bridge
- Designated port

The following table describes the STP parameters.

**Table 22** STP parameters

Parameters	Description
Current Root	Shows information about the root bridge for the Spanning Tree. Information includes the priority (hex) and MAC address of the root.
Path-Cost	Path-cost is the total path cost to the root bridge. It is the summation of the path cost between bridges (up to the root bridge).
Port	The current root port refers to the port on the switch that receives data from the current root. Zero (0) indicates the root bridge of the STP.
Priority (bridge)	The bridge priority parameter controls which bridge on the network will become the STP root bridge.
Hello	The hello time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
MaxAge	The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the STP network. If the bridge is not the root bridge, it uses the MaxAge value of the root bridge.
FwdDel	The forward delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from learning state to forwarding state. If the bridge is not the root bridge, it uses the FwdDel value of the root bridge.
Aging	The aging time parameter specifies, in seconds, the amount of time the bridge waits without receiving a packet from a station before removing the station from the Forwarding Database.
Priority (port)	The port priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
Cost	The port path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost.
State	The State field shows the current state of the port. The State field can be one of the following: BLOCKING, LISTENING, LEARNING, FORWARDING, or DISABLED.
Designated bridge	Shows information about the bridge connected to each port, if applicable. Information includes the priority (hex) and MAC address of the Designated Bridge.
Designated port	The port ID of the port on the Designated Bridge to which this port is connected. This information includes the port priority (hex) and the port number (hex).

## Rapid Spanning Tree / Multiple Spanning Tree information

**Command:** /info/l2/stp

```
-----
upfast disabled, update 40
BPDU Guard disabled
Pvst+ compatibility mode enabled
-----

Spanning Tree Group 1: On (RSTP)
VLANs: 1-3

Current Root:          Path-Cost   Port Hello MaxAge FwdDel
8000 00:00:01:00:19:00      0       0    9    20    15

Parameters:  Priority   Hello   MaxAge   FwdDel   Aging
              32768      9       20       15      300

Port  Prio  Cost   State  Role  Designated Bridge  Des Port  Type
-----
  1    0    0      DSB
  2    0    0      DSB
  3    0    0      DSB
  4    0    0      DSB
  5    0    0      DSB
  6    0    0      DSB
  7    0    0      DSB
  8    0    0      DSB
  9    0    0      DSB
 10    0    0      DISC
 11    0    0      FWD   DESG  8000-00:00:01:00:19:00  8017  P2P2, Edge
 12    0    0      FWD   DESG  8000-00:00:01:00:19:00  8018  P2P
```

The switch software can be set to use the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) or the IEEE 802.1s Multiple Spanning Tree Protocol (MSTP). If RSTP/MSTP is turned on, you can view the following RSTP bridge information for the Spanning Tree Group:

- Status of Uplink Fast (upfast)
- Current root MAC address
- Path-Cost
- Port
- Hello interval
- Maximum age value
- Forwarding delay
- Aging time

You can also refer to the following port-specific RSTP information:

- Port number and priority
- Cost
- State
- Role
- Designated bridge and port
- Link type

The following table describes the STP parameters in RSTP or MSTP mode.

**Table 23** Rapid Spanning Tree parameter descriptions

Parameter	Description
Current Root	Shows information about the root bridge for the Spanning Tree. Information includes the priority (hex) and MAC address of the root.
Path-Cost	Path-cost is the total path cost to the root bridge. It is the summation of the path cost between bridges (up to the root bridge).
Port	The current root port refers to the port on the switch that receives data from the current root. Zero (0) indicates the root bridge of the STP.
Priority (bridge)	The bridge priority parameter controls which bridge on the network will become the STP root bridge.
Hello	The hello time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
MaxAge	The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the STP network. If the bridge is not the root bridge, it uses the MaxAge value of the root bridge.
FwdDel	The forward delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from learning state to forwarding state. If the bridge is not the root bridge, it uses the FwdDel value of the root bridge.
Aging	The aging time parameter specifies, in seconds, the amount of time the bridge waits without receiving a packet from a station before removing the station from the Forwarding Database.
Priority (port)	The port priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
Cost	The port path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of zero (0) indicates that the cost will be set to the appropriate default after the link speed has been auto-negotiated.
State	Shows the current state of the port. The State field in RSTP/MSTP mode can be one of the following: Discarding (DISC), Learning (LRN), Forwarding (FWD), or Disabled (DSB).
Role	Shows the current role of this port in the Spanning Tree. The port role can be one of the following: Designated (DESG), Root (ROOT), Alternate (ALTN), Backup (BKUP), Master (MAST), or Unknown (UNK).
Designated bridge	Shows information about the bridge connected to each port, if applicable. Information includes the priority (hex) and MAC address of the Designated Bridge.
Designated port	The port ID of the port on the Designated Bridge to which this port is connected.
Type	Type of link connected to the port, and whether the port is an edge port. Link type values are AUTO, P2P, or SHARED. MSTP: The Type field appears in /info/cist.

# Common Internal Spanning Tree information

**Command:** /info/l2/cist

```
Mstp Digest: 0xac36177f50283cd4b83821d8ab26de62
Common Internal Spanning Tree:
VLANs MAPPED: 1-16 18-31 33-4094
VLANs: 1 25 26 4095

Current Root:          Path-Cost  Port    MaxAge  FwdDel
8000 00:03:42:fa:3b:80      0        1       20     15

CIST Regional Root:    Path-Cost
8000 00:03:42:fa:3b:81     11

Parameters:  Priority  MaxAge  FwdDel  Hops
              32768    20      15     20

Port Prio Cost State  Role Designated Bridge      Des Port Hello Type
-----
  1  128  2000   FWD   DESG 8000-00:03:42:fa:3b:80  8001    4  P2P, Edge
  2  128  2000   FWD   DESG 8000-00:03:42:fa:3b:80  8002
  3  128  2000   DSB
  4  128  2000   DSB
  5  128  2000   DSB
  6  128  2000   DSB
  7  128  2000   DSB
  8  128  2000   DSB
  9  128  2000   DSB
 10  128    0   DSB
 11  128  2000   FWD   DESG 8000-00:03:42:fa:3b:80
 12  128  2000   DSB
...
```

In addition to seeing if Common Internal Spanning Tree (CIST) is enabled or disabled, you can view the following CIST bridge information:

- Status of Uplink Fast (upfast)
- CIST root
- CIST regional root
- Priority
- Maximum age value
- Forwarding delay
- Hops

You can also refer to the following port-specific CIST information:

- Port number and priority
- Cost
- State
- Role
- Designated bridge and port
- Hello interval
- Link type and port type

The following table describes the CIST parameters.

**Table 24** Common Internal Spanning Tree parameter description

Parameter	Description
CIST Root	Shows information about the root bridge for the Common Internal Spanning Tree (CIST). Values on this row of information refer to the CIST root.
CIST Regional Root	Shows information about the root bridge for this MSTP region. Values on this row of information refer to the regional root.
Priority (bridge)	The bridge priority parameter controls which bridge on the network will become the STP root bridge.
MaxAge	The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the STP network.
FwdDel	The forward delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from learning state to forwarding state.
Hops	Shows the maximum number of bridge hops allowed before a packet is dropped.
Priority (port)	The port priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
Cost	The port path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of zero (0) indicates that the cost will be set to the appropriate default after the link speed has been auto-negotiated.
State	Shows the current state of the port. The state field can be one of the following: Discarding (DISC), Forwarding (FWD), or Disabled (DSB).
Role	Shows the current role of this port in the Spanning Tree. The port role can be one of the following: Designated (DESG), Root (ROOT), Alternate (ALTN), Backup (BKUP), Master (MAST).
Designated Bridge	Shows information about the bridge connected to each port, if applicable. Information includes the priority (hex) and MAC address of the Designated Bridge.
Designated Port	The port ID of the port on the Designated Bridge to which this port is connected. Information includes the port priority (hex) and the port number (hex).
Hello	The hello time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
Type	Type of link connected to the port, and whether the port is an edge port. Link type values are AUTO, P2P, or SHARED.

## Trunk group information

**Command:** /info/l2/trunk

```
Trunk group 1, Enabled
port state:
  20: STG  1 forwarding
  21: STG  1 forwarding
```

When trunk groups are configured, you can view the state of each port in the various trunk groups.

**NOTE:** If Spanning Tree Protocol on any port in the trunk group is set to forwarding, the remaining ports in the trunk group will also be set to forwarding.

## VLAN information

**Command:** /info/l2/vlan

VLAN	Name			Status	Ports	
1	Default VLAN			ena	4 5	
2	pc03p			ena	2	
7	pc07f			ena	7	
11	pc04u			ena	11	
14	8600-14			ena	14	
15	8600-15			ena	15	
16	8600-16			ena	16	
17	8600-17			ena	6	
18	35k-1			ena	18	
19	35k-2			ena	19	
20	35k-3			ena	20	
21	35k-4			ena	21	
22	pc07z			ena	21	
24	redlan			ena	21	
300	ixiaTraffic			ena	1 12 13 23	
4000	bpsports			ena	3-6 8-10	
4095	Mgmt VLAN			ena	17	
PVLAN	Protocol	FrameType	EtherType	Priority	Status	Ports
1	1	Ether2	0080	0	ena	4
PVLAN	PVLAN-Tagged Ports					
none	none					
Private-VLAN	Type	Mapped-To	Status	Ports		
20	primary	empty	ena	empty		



This information display includes all configured VLANs and all member ports that have an active link state.

VLAN information includes:

- VLAN Number
- VLAN Name
- Status
- Port membership of the VLAN
- Protocol VLAN information
- Private VLAN information

## Fast Uplink Convergence status

**Command:** /info/l2/uplink

```
STP uplink fast mode : disabled
```

The following table describes the status of Fast Uplink Convergence.

**Table 25** L2 general information

Field	Description
STP uplink fast mode	Displays the status of STP Uplink Fast: enabled or disabled.

# Layer 3 information

**Command:** /info/l3

```
[Layer 3 Menu]
route    - IP Routing Information Menu
arp      - ARP Information Menu
ospf     - OSPF Routing Information Menu
rip      - RIP Routing Information Menu
ip       - Show IP information
igmp     - Show IGMP Snooping Multicast Group information
vrrp     - Show Virtual Router Redundancy Protocol information
sm       - Server Mobility Information Menu
dump     - Dump all layer 3 information
```

The following table describes the Layer 3 Information Menu options.

**Table 26** Layer 3 Information Menu options

Command	Usage
route	Displays the IP Routing Menu. Using the options of this menu, the system displays the following for each configured or learned route: <ul style="list-style-type: none"><li>• Route destination IP address, subnet mask, and gateway address</li><li>• Type of route</li><li>• Tag indicating origin of route</li><li>• Metric for RIP tagged routes, specifying the number of hops to the destination (1-15 hops, or 16 for infinite hops)</li><li>• The IP interface that the route uses</li></ul>
arp	Displays the Address Resolution Protocol (ARP) Information Menu.
ospf	Displays OSPF routing Information Menu.
rip	Displays Routing Information Protocol Menu.
ip	Displays IP Information. IP information, includes: <ul style="list-style-type: none"><li>• IP interface information: Interface number, IP address, subnet mask, VLAN number, and operational status.</li><li>• Default gateway information: Metric for selecting which configured gateway to use, gateway number, IP address, and health status</li><li>• IP forwarding information: Enable status, Inet and lmask</li><li>• Port status</li></ul>
igmp	Displays IGMP Information Menu.
vrrp	Displays the VRRP Information Menu.
sm	Displays the Server Mobility Information Menu.
dump	Dumps all switch information available from the Layer 3 Menu (10K or more, depending on your configuration).  If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.

## Route information

**Command:** /info/l3/route

```
[IP Routing Menu]
  find      - Show a single route by destination IP address
  gw        - Show routes to a single gateway
  type      - Show routes of a single type
  tag       - Show routes of a single tag
  if        - Show routes on a single interface
  dump      - Show all routes
```

Using the commands listed below, you can display all or a portion of the IP routes currently held in the switch.

**Table 27** Route Information menu options

Command	Usage
find <IP address>	Displays a single route by IP address. For example, 100.10.1.1.
gw <IP address>	Displays routes to a single gateway. For example, 100.10.1.2.
type indirect direct local broadcast martian multicast	Displays routes of a single type.
tag fixed static addr rip ospf broadcast martian multicast	Displays routes of a single tag.
if <1-250>	Displays routes on a single interface.
dump	Displays all routes configured in the switch.

## Show all IP Route information

**Command:** /info/l3/route/dump

```
Status code: * - best
Destination      Mask           Gateway        Type           Tag           Metr If
-----
* 11.0.0.0        255.0.0.0      11.0.0.1       direct         fixed          211
* 11.0.0.1        255.255.255.255 11.0.0.1       local          addr           211
* 11.255.255.255  255.255.255.255 11.255.255.255 broadcast      broadcast      211
* 12.0.0.0        255.0.0.0      12.0.0.1       direct         fixed          12
* 12.0.0.1        255.255.255.255 12.0.0.1       local          addr           12
* 12.255.255.255  255.255.255.255 12.255.255.255 broadcast      broadcast      12
* 13.0.0.0        255.0.0.0      11.0.0.2       indirect       ospf           2    211
* 47.0.0.0        255.0.0.0      47.133.88.1    indirect       static         24
* 47.133.88.0     255.255.255.0  47.133.88.46   direct         fixed          24
* 172.30.52.223   255.255.255.255 172.30.52.223  broadcast     broadcast      2
* 224.0.0.0       224.0.0.0      0.0.0.0        martian        martian
* 224.0.0.5       255.255.255.255 0.0.0.0        multicast      addr
```

The following table describes the Type parameter.

**Table 28** IP Routing Type information

Field	Description
indirect	The next hop to the host or subnet destination will be forwarded through a router at the Gateway address.
direct	Packets will be delivered to a destination host or subnet attached to the switch.
local	Indicates a route to one of the switch's IP interfaces.
broadcast	Indicates a broadcast route.
martian	The destination belongs to a host or subnet which is filtered out. Packets to this destination are discarded.
multicast	Indicates a multicast route.

The following table describes the Tag parameter.

**Table 29** IP Routing Tag information

Field	Description
fixed	The address belongs to a host or subnet attached to the switch.
static	The address is a static route which has been configured on the switch.
addr	The address belongs to one of the switch's IP interfaces.
rip	The address was learned by the Routing Information Protocol (RIP).
ospf	The address was learned by Open Shortest Path First (OSPF).
broadcast	Indicates a broadcast address.
martian	The address belongs to a filtered group.

## ARP information

**Command:** /info/arp

```
[Address Resolution Protocol Menu]
  find      - Show a single ARP entry by IP address
  port      - Show ARP entries on a single port
  vlan      - Show ARP entries on a single VLAN
  addr      - Show ARP entries for switch's interfaces
  dump      - Show all ARP entries
```

The Address Resolution Protocol (ARP) information includes IP address and MAC address of each entry, address status flags, VLAN, and port for the address, and port referencing information.

The following table describes the Address Resolution Protocol Menu options.

**Table 30** ARP information

Command	Usage
find <IP address>	Displays a single ARP entry by IP address. For example, 192.4.17.101.
port <port number>	Displays the ARP entries on a single port.
vlan <1-4095>	Displays the ARP entries on a single VLAN.
addr	Displays the ARP address list: IP address, IP mask, MAC address, and VLAN flags.
dump	Displays all ARP entries, including: <ul style="list-style-type: none"><li>• IP address and MAC address of each entry</li><li>• Address status flag</li><li>• The VLAN and port to which the address belongs</li><li>• The ports which have referenced the address (empty if no port has routed traffic to the IP address shown)</li></ul>

## Show all ARP entry information

**Command:** /info/arp/dump

IP address	Flags	MAC address	VLAN	Port
-----	-----	-----	----	----
192.168.2.4		00:50:8b:b2:32:cb	1	18
192.168.2.19		00:0e:7f:25:89:b5	1	17
192.168.2.61	P	00:0f:6a:ed:46:00	1	

The Flag field provides additional information about an entry. If no flag displays, the entry is normal.

**Table 31** ARP dump flag parameters

Flag	Description
P	Permanent entry created for switch IP interface.
R	Indirect route entry.
U	Unresolved ARP entry. The MAC address has not been learned.

## ARP address list information

**Command:** /info/arp/addr

IP address	IP mask	MAC address	VLAN	Flags
-----	-----	-----	----	-----
205.178.18.66	255.255.255.255	00:70:cf:03:20:04		P
205.178.50.1	255.255.255.255	00:70:cf:03:20:06	1	
205.178.18.64	255.255.255.255	00:70:cf:03:20:05	1	

This screen displays all entries in the ARP cache.

## OSPF information

**Command:** /info/l3/ospf

```
[OSPF Information Menu]
  general - Show general information
  aindex  - Show area(s) information
  if      - Show interface(s) information
  virtual - Show details of virtual links
  nbr     - Show neighbor(s) information
  dbase   - Database Menu
  sumaddr - Show summary address list
  nsumadd - Show NSSA summary address list
  routes  - Show OSPF routes
  dump    - Show OSPF information
```

The following table describes the OSPF Menu options.

**Table 32** OSPF information

Command	Usage
general	Displays general OSPF information.
aindex <0-2>	Displays area information for a particular area index. If no parameter is supplied, it displays area information for all the areas.
if <1-249>	Displays interface information for a particular interface. If no parameter is supplied, it displays information for all the interfaces.
virtual	Displays information about all the configured virtual links.
nbr <nbr router-id (A.B.C.D)>	Displays the status of a neighbor with a particular router ID. If no router ID is supplied, it displays the information about all the current neighbors.
dbase	Displays OSPF database menu.
sumaddr <0-2>	Displays the list of summary ranges belonging to non-NSSA areas.
nsumadd <0-2>	Displays the list of summary ranges belonging to NSSA areas.
routes	Displays OSPF routing table.
dump	Displays all OSPF information.

## OSPF general information

**Command:** /info/l3/ospf/general

```
OSPF Version 2
Router ID: 10.10.10.1
Started at 1663 and the process uptime is 4626
Area Border Router: yes, AS Boundary Router: no
LS types supported are 6
External LSA count 0
External LSA checksum sum 0x0
Number of interfaces in this router is 2
Number of virtual links in this router is 1
16 new lsa received and 34 lsa originated from this router
Total number of entries in the LSDB 10
Database checksum sum 0x0
Total neighbors are 1, of which
                                2 are >=INIT state,
                                2 are >=EXCH state,
                                2 are =FULL state
Number of areas is 2, of which 3-transit 0-nssa 0-stub
    Area Id : 0.0.0.0
    Authentication : none
    Import ASExtern : yes
    Number of times SPF ran : 8
    Area Border Router count : 2
    AS Boundary Router count : 0
    LSA count : 5
    Summary : noSummary
```

## OSPF interface information

**Command:** /info/l3/ospf/if

```
Ip Address 10.10.12.1, Area 0.0.0.1, Admin Status UP
Router ID 10.10.10.1, State DR, Priority 1
Designated Router (ID) 10.10.10.1, Ip Address 10.10.12.1
Backup Designated Router (ID) 10.10.14.1, Ip Address 10.10.12.2
Timer intervals, Hello 10, Dead 40, Wait 40, Retransmit 5,
Transit delay 1
Neighbor count is 1 If Events 4, Authentication type none
```

## OSPF Database information menu

**Command:** /info/l3/ospf/dbase

```
[OSPF Database Menu]
advrtr    - LS Database info for an Advertising Router
asbrsum   - ASBR Summary LS Database info
dbsumm    - LS Database summary
ext       - External LS Database info
nw        - Network LS Database info
nssa      - NSSA External LS Database info
rtr       - Router LS Database info
self      - Self Originated LS Database info
summ      - Network-Summary LS Database info
all       - All
```

The following table describes the OSPF Database information menu options.

**Table 33** OSPF Database information

Command	Usage
advrtr <router-id (A.B.C.D)>	Takes advertising router as a parameter. Displays all the Link State Advertisements (LSAs) in the LS database that have the advertising router with the specified router ID, for example: 20.1.1.1.
asbrsum <adv-rtr (A.B.C.D)> <link_state_id (A.B.C.D)> <self>	Displays ASBR summary LSAs. The usage of this command is as follows: <ul style="list-style-type: none"><li>• asbrsum adv-rtr 20.1.1.1 displays ASBR summary LSAs having the advertising router 20.1.1.1.</li><li>• asbrsum link_state_id 10.1.1.1 displays ASBR summary LSAs having the link state ID 10.1.1.1.</li><li>• asbrsum self displays the self advertised ASBR summary LSAs.</li><li>• asbrsum with no parameters displays all the ASBR summary LSAs.</li></ul>
dbsumm	Displays the following information about the LS database in a table format: <ul style="list-style-type: none"><li>• The number of LSAs of each type in each area.</li><li>• The total number of LSAs for each area.</li><li>• The total number of LSAs for each LSA type for all areas combined.</li><li>• The total number of LSAs for all LSA types for all areas combined.</li></ul> No parameters are required.
ext <adv-rtr (A.B.C.D)> <link_state_id (A.B.C.D)> <self>	Displays the AS-external (type 5) LSAs with detailed information of each field of the LSAs. The usage of this command is the same as the usage of the command asbrsum.
nw <adv-rtr (A.B.C.D)> <link_state_id (A.B.C.D)> <self>	Displays the network (type 2) LSAs with detailed information of each field of the LSA.network LS database. The usage of this command is the same as the usage of the command asbrsum.
nssa <adv-rtr (A.B.C.D)> <link_state_id (A.B.C.D)> <self>	Displays the NSSA (type 7) LSAs with detailed information of each field of the LSAs. The usage of this command is the same as the usage of the command asbrsum.



**Table 33** OSPF Database information

Command	Usage
<code>rtr &lt;adv-rtr (A.B.C.D)&gt; &lt;link_state_id (A.B.C.D)&gt; &lt;self&gt;</code>	Displays the router (type 1) LSAs with detailed information of each field of the LSAs. The usage of this command is the same as the usage of the command <code>asbrsum</code> .
<code>self</code>	Displays all the self-advertised LSAs. No parameters are required.
<code>summ &lt;adv-rtr (A.B.C.D)&gt; &lt;link_state_id (A.B.C.D)&gt; &lt;self&gt;</code>	Displays the network summary (type 3) LSAs with detailed information of each field of the LSAs.  The usage of this command is the same as the usage of the command <code>asbrsum</code> .
<code>all</code>	Displays all the LSAs.

## OSPF route codes information

**Command:** `/info/l3/ospf/routes`

```
Codes: IA - OSPF inter area,
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
* - best

IA 10.10.0.0/16 via 200.1.1.2
IA 40.1.1.0/28 via 20.1.1.2
IA 80.1.1.0/24 via 200.1.1.2
IA 100.1.1.0/24 via 20.1.1.2
IA 140.1.1.0/27 via 20.1.1.2
IA 150.1.1.0/28 via 200.1.1.2
E2 172.18.1.1/32 via 30.1.1.2
E2 172.18.1.2/32 via 30.1.1.2
E2 172.18.1.3/32 via 30.1.1.2
E2 172.18.1.4/32 via 30.1.1.2
E2 172.18.1.5/32 via 30.1.1.2
E2 172.18.1.6/32 via 30.1.1.2
E2 172.18.1.7/32 via 30.1.1.2
E2 172.18.1.8/32 via 30.1.1.2
```

## Routing Information Protocol information

**Command:** /info/l3/rip

```
[RIP Information Menu]
  routes    - Show RIP routes
  dump      - Show RIP user's configuration
```

The following table describes the Routing Information Protocol information menu options.

**Table 34** RIP information

Command	Usage
routes	Displays information about RIP routes.
dump <0-249>	Displays RIP user's configuration. Enter 0 (zero) for all interfaces.

## RIP Routes information

**Command:** /info/l3/rip/routes

```
>> IP Routing# /info/l3/rip/routes

3.0.0.0/8 via 30.1.1.11 metric 4
4.0.0.0/16 via 30.1.1.11 metric 16
10.0.0.0/8 via 30.1.1.2 metric 3
20.0.0.0/8 via 30.1.1.2 metric 2
```

This table contains all dynamic routes learned through RIP, including the routes that are undergoing garbage collection with metric = 16. This table does not contain directly connected routes and locally configured static routes.

## RIP user configuration

**Command:** /info/l3/rip/dump <1-249>

```
RIP USER CONFIGURATION :
RIP on update 30
RIP Interface 2 : 102.1.1.1, enabled
version 2, listen enabled, supply enabled, default none
poison disabled, trigg enabled, mcast enabled, metric 1
auth none, key none
RIP Interface 3 : 103.1.1.1, enabled
version 2, listen enabled, supply enabled, default none
poison disabled, trigg enabled, mcast enabled, metric 1
```

## IP information

**Command:** /info/l3/ip

```
IP information:
Interface information:
  1: 10.80.23.243      255.255.254.0    10.80.23.255,    vlan 1, up
 250: 10.20.7.144      255.255.0.0      10.20.255.255,   vlan 4095, up

Default gateway information: metric strict
  1: 10.80.22.1,      vlan any, up active
 254: 10.20.1.1,      vlan 4095, up active

Current ServerMobility settings: OFF
ServerMobility ports: empty
DHCP request filtering enabled ports: empty
Relay on non-ServerMobility ports: Ena
Active-Backup ports:
Current IP forwarding settings: OFF, dirbr disabled

Current network filter settings:
  none

Current route map settings:
```

The following interface and default gateway information is displayed:

- Interface number
- IP address
- IP mask
- IP broadcast address
- Operational status
- BootP relay settings
- Server Mobility settings
- IP forwarding settings
- Network filter settings
- Route map settings

## IGMP multicast group information

**Command:** /info/l3/igmp

```
[IGMP Multicast Group Menu]
mrouter - Show IGMP Snooping Multicast Router Port information
find     - Show a single group by IP group address
vlan     - Show groups on a single vlan
port     - Show groups on a single port
trunk    - Show groups on a single trunk
detail   - Show detail of a single group by IP group address
dump     - Show all groups
```

The following table describes the commands used to display information about IGMP groups learned by the switch.

**Table 35** IGMP Multicast Group menu options

Command	Usage
mrouter	Displays the Multicast Router Menu.
find <IP address>	Displays a single IGMP multicast group by its IP address.
vlan <1-4094>	Displays all IGMP multicast groups on a single VLAN.
port <port number>	Displays all IGMP multicast groups on a single port.
trunk <1-40>	Displays all IGMP multicast groups on a single trunk group.
detail	Displays details about IGMP multicast groups, including source and timer information.
dump	Displays information for all multicast groups.

## IGMP group information

**Command:** /info/l3/igmp/dump

```
Note: Local groups (224.0.0.x) are not snooped/relayed and will not appear.
Source      Group      VLAN    Port    Version  Mode  Expires  Fwd
-----
10.1.1.1    232.1.1.1    2       21      V3       INC   4:16     Yes
10.1.1.5    232.1.1.1    2       21      V3       INC   4:16     Yes
*           232.1.1.1    2       21      V3       INC   -        No
10.10.10.43 235.0.0.1    9       21      V3       INC   2:26     Yes
*           236.0.0.1    9       21      V3       EXC   -        Yes
```

IGMP Group information includes:

- IGMP source address
- IGMP Group address
- VLAN and port
- IGMP version
- IGMPv3 filter mode
- Expiration timer value
- IGMP multicast forwarding state

## IGMP multicast router information

**Command:** /info/l3/igmp/mrouter

[IGMP Multicast Router Menu]

vlan - Show all multicast router ports on a single vlan

dump - Show all learned multicast router ports

The following table describes the commands used to display information about multicast routers learned through IGMP Snooping.

**Table 36** IGMP Multicast Router menu options

Command	Usage
vlan <1-4094>	Displays information for all multicast groups on a single VLAN.
dump	Displays information for all multicast groups learned by the switch.

## VRRP information

Virtual Router Redundancy Protocol (VRRP) support on the HP 10GbE switch provides redundancy between routers in a LAN. This is accomplished by configuring the same virtual router IP address and ID number on each participating VRRP-capable routing device. One of the virtual routers is then elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will assume routing authority and take control of the virtual router IP address.

**Command:** `/info/l3/vrrp`

```
VRRP information:
1: vrid 2, 205.178.18.210, if 1, renter, prio 100, master, server
2: vrid 1, 205.178.18.202, if 1, renter, prio 100, backup
3: vrid 3, 205.178.18.204, if 1, renter, prio 100, master, proxy
```

When virtual routers are configured, you can view the status of each virtual router using this command. VRRP information includes:

- Virtual router number
- Virtual router ID and IP address
- Interface number
- Ownership status
  - `owner` identifies the preferred master virtual router. A virtual router is the owner when the IP address of the virtual router and its IP interface are the same.
  - `renter` identifies virtual routers which are not owned by this device
- Priority value. During the election process, the virtual router with the highest priority becomes master.
- Activity status
  - `master` identifies the elected master virtual router.
  - `backup` identifies that the virtual router is in backup mode.
  - `init` identifies that the virtual router is waiting for a startup event. Once it receives a startup event, it transitions to master if its priority is 255, (the IP address owner), or transitions to backup if it is not the IP address owner.
- Server status. The `server` state identifies virtual routers.
- Proxy status. The proxy state identifies virtual proxy routers, where the virtual router shares the same IP address as a proxy IP address. The use of virtual proxy routers enables redundant switches to share the same IP address, minimizing the number of unique IP addresses that must be configured.

## Server Mobility Port information

**Command:** /info/13/sm/port

```
-----  
Server Mobility Port 2 Information:  
  
agent.circuit-id = 55:53:45:36:33:35:31:4d:34:36:00:00:00:00:00  
agent.remote-id  = 02:00:00:00:02  
Server Mobility : enabled  
      Filtering  : enabled  
Port 2 has no backup port
```

This display includes the following information for each port that has Server Mobility configured:

- Agent Circuit ID—hexadecimal value of the DHCP option 82 Agent Circuit ID
- Agent Remote ID—hexadecimal value of the DHCP option 82 Agent Remote ID
- Server Mobility status (enabled or disabled)
- Status of Server Mobility filtering
- Backup port

## QoS information

**Command:** /info/qos

```
[QoS Menu]
8021p      - Show QOS 802.1p information
```

The following table describes the commands used to display Quality of Service (QoS) information.

**Table 37** QoS menu options

Command	Usage
8021p	Displays the QoS 802.1p Information Menu.

## 802.1p information

**Command:** /info/qos/8021p

Current priority to COS queue information:

Priority	COSq	Weight
----------	------	--------

0	0	1
1	0	1
2	0	1
3	0	1
4	1	2
5	1	2
6	1	2
7	1	2

Current port priority information:

Port	Priority	COSq	Weight
------	----------	------	--------

1	0	0	1
2	0	0	1
3	0	0	1
4	0	0	1
...			
20	0	0	1
21	0	0	1

The following table describes the IEEE 802.1p priority to COS queue information.

**Table 38** 802.1p Priority to COS Queue information

Field	Description
Priority	Displays the 802.1p Priority level.
Cosq	Displays the Class of Service queue.
Weight	Displays the scheduling weight of the COS queue.



The following table describes the IEEE 802.1p port priority information.

**Table 39** 802.1p Port Priority information

Field	Description
Port	Displays the port number.
Priority	Displays the 802.1p Priority level.
Cosq	Displays the Class of Service queue.
Weight	Displays the scheduling weight.

## ACL information

**Command:** /info/acl

```
Current ACL information:
-----
Filter 1 profile:
  Ethernet
    - VID      : 1/0xffff
    Actions    : Set COS to 0
Filter 2 profile:
  Ethernet
    - VID      : 1/0xffff
    Actions    : Permit
No ACL groups configured.
```

Access Control List (ACL) information provides configuration parameters for each Access Control List. It also shows which ACLs are included in each ACL Group.

# RMON Information Menu

**Command:** /info/rmon

```
[RMON Information Menu]
  hist    - Show RMON History group information
  alarm   - Show RMON Alarm group information
  event   - Show RMON Event group information
  dump    - Show all RMON information
```

The following table describes the RMON Information parameters.

**Table 40** RMON History Information Menu

Command	Usage
hist	Displays the RMON History Information menu.
alarm	Displays the RMON Alarm Information menu.
event	Displays the RMON Event Information menu.
dump	Displays all RMON Information parameters.

## RMON history information

**Command:** /info/rmon/hist

RMON History group configuration:

Index	IFOID	Interval	Rbnum	Gbnum
1	1.3.6.1.2.1.2.2.1.1.21	30	5	5
2	1.3.6.1.2.1.2.2.1.1.18	30	5	5
3	1.3.6.1.2.1.2.2.1.1.20	30	5	5
4	1.3.6.1.2.1.2.2.1.1.19	30	5	5
5	1.3.6.1.2.1.2.2.1.1.21	1800	5	5

The following table describes the RMON History Information parameters.

**Table 41** RMON History Information Menu

Field	Description
Index	Displays the index number that identifies each history instance.
IFOID	Displays the MIB Object Identifier.
Interval	Displays the time interval for each sampling bucket.
Rbnum	Displays the number of requested buckets, which is the number of data slots into which data is to be saved.
Gbnum	Displays the number of granted buckets that may hold sampled data.

## RMON alarm information

**Command:** /info/rmon/alarm

RMON Alarm group configuration:

Index	Interval	Type	rLimit	fLimit	rEvtIdx	fEvtIdx	last value
1	30	abs	10	0	1	0	0
2	900	abs	0	10	0	2	0
3	300	abs	10	20	0	0	0
4	1800	abs	10	0	1	0	0
5	1800	abs	10	0	1	0	0
8	1800	abs	10	0	1	0	56344540
10	1800	abs	10	0	1	0	0
11	1800	abs	10	0	1	0	0
15	1800	abs	10	0	1	0	0
18	1800	abs	10	0	1	0	0
100	1800	abs	10	0	1	0	0

Index	OID
1	1.3.6.1.2.1.2.2.1.10.257
2	1.3.6.1.2.1.2.2.1.11.258
3	1.3.6.1.2.1.2.2.1.12.259
4	1.3.6.1.2.1.2.2.1.13.260
5	1.3.6.1.2.1.2.2.1.14.261
8	1.3.6.1.2.1.2.2.1.10.271
10	1.3.6.1.2.1.2.2.1.15.262
11	1.3.6.1.2.1.2.2.1.16.263
15	1.3.6.1.2.1.2.2.1.19.266
18	1.3.6.1.2.1.2.2.1.10.270
100	1.3.6.1.2.1.2.2.1.17.264

The following table describes the RMON Alarm Information parameters.

**Table 42** RMON Alarm Information Menu

Field	Description
Index	Displays the index number that identifies each alarm instance.
Interval	Displays the time interval over which data is sampled and compared with the rising and falling thresholds.
Type	Displays the method of sampling the selected variable and calculating the value to be compared against the thresholds, as follows: <ul style="list-style-type: none"> <li>abs—absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval.</li> <li>delta—delta value, the value of the selected variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.</li> </ul>
rLimit	Displays the rising threshold for the sampled statistic.
fLimit	Displays the falling threshold for the sampled statistic.
rEvtIdx	Displays the rising alarm event index that is triggered when a rising threshold is crossed.
fEvtIdx	Displays the falling alarm event index that is triggered when a falling threshold is crossed.

**Table 42** RMON Alarm Information Menu

Field	Description
Last value	Displays the last sampled value.
OID	Displays the MIB Object Identifier for each alarm index.

## RMON event information

**Command:** /info/rmon/event

RMON Event group configuration:

Index	Type	Last Sent	Description
1	both	0D: 0H: 1M:20S	Event_1
2	none	0D: 0H: 0M: 0S	Event_2
3	log	0D: 0H: 0M: 0S	Event_3
4	trap	0D: 0H: 0M: 0S	Event_4
5	both	0D: 0H: 0M: 0S	Log and trap event for Link Down
10	both	0D: 0H: 0M: 0S	Log and trap event for Link Up
11	both	0D: 0H: 0M: 0S	Send log and trap for icmpInMsg
15	both	0D: 0H: 0M: 0S	Send log and trap for icmpInEchos
100	both	0D: 0H: 0M: 0S	Event 100

The following table describes the RMON Event Information parameters.

**Table 43** RMON Event Information Menu

Field	Description
Index	Displays the index number that identifies each event instance.
Type	Displays the type of notification provided for this event, as follows: none, log, trap, both.
Last Sent	Displays the time that passed since the last switch reboot, when the most recent event was triggered. This value is cleared when the switch reboots.
Description	Displays a text description of the event.

# Link status information

**Command:** /info/link

-----					
Port	Speed	Duplex	Flow Ctrl		Link
----	-----	-----	--TX--	RX--	-----
1	10000	full	yes	yes	down
2	10000	full	yes	yes	down
3	10000	full	yes	yes	down
4	10000	full	yes	yes	down
5	10000	full	yes	yes	down
6	10000	full	yes	yes	down
7	10000	full	yes	yes	down
8	10000	full	yes	yes	down
9	10000	full	yes	yes	up
10	10000	full	yes	yes	down
11	10000	full	yes	yes	down
12	10000	full	yes	yes	down
13	10000	full	yes	yes	down
14	10000	full	yes	yes	down
15	10000	full	yes	yes	down
16	10000	full	yes	yes	down
17	100	full	yes	yes	up
18	10000	full	yes	yes	down
19	10000	full	yes	yes	down
20	10000	full	yes	yes	down
21	10000	full	yes	yes	down

Use this command to display link status information about each port on a switch, including:

- Port number
- Port speed (10000 Mb/s or 100 Mb/s)
- Duplex mode (half, full, or any)
- Flow control for transmit and receive (no, yes, or any)
- Link status (up, down, or disabled)

# Port information

**Command:** /info/port

Port	Tag	RMON	PVID	NAME	VLAN(s)
1	n	d	1	Downlink1	1
2	n	d	1	Downlink2	1
3	n	d	1	Downlink3	1
4	n	d	1	Downlink4	1
5	n	d	1	Downlink5	1
6	n	d	1	Downlink6	1
7	n	d	1	Downlink7	1
8	n	d	1	Downlink8	1
9	n	d	1	Downlink9	1
10	n	d	1	Downlink10	1
11	n	d	1	Downlink11	1
12	n	d	1	Downlink12	1
13	n	d	1	Downlink13	1
14	n	d	1*	Downlink14	1
15	n	d	1*	Downlink15	1
16	n	d	1*	Downlink16	1
17	n	d	4095	Mgmt	4095
18	n	d	1*	Uplink1	1
19	n	d	1*	Uplink2	1
20	n	d	1*	Uplink3	1
21	n	d	1*	Uplink4	1

\* = PVID is tagged.

Port information includes:

- Port number
- Whether the port uses VLAN tagging or not (y or n)
- Whether Remote Monitoring (RMON) is enabled or disabled (e or d)
- Port VLAN ID (PVID)
- Port name
- VLAN membership

# Transceiver status

**Command:** /info/transcvr

Port	Device	TX-Enable	RX-Signal	TX-Fault
XFP1	SR-XFP	enabled	ok	N/A
XFP2	SR-XFP	enabled	LOST	N/A
XFP3	SR-XFP	enabled	ok	N/A
XFP4	SR-XFP	****	NOT Installed	****

This command displays the status of the Small Form Pluggable (SFP) module on each Fiber External Port.

# Uplink Failure Detection information

**Command:** /info/ufd

```
Uplink Failure Detection: Enabled
LtM status: Down
Member      STG      STG State      Link Status
-----
port 20
           1      DISABLED
           10     DISABLED *
           15     DISABLED *
* = STP turned off for this port.

LtD status: Auto Disabled
Member      Link Status
-----
port 1      disabled
port 2      disabled
port 3      disabled
port 4      disabled
```

Uplink Failure Detection (UFD) information includes:

- UFD status, either enabled or disabled
- LtM status and member ports
- Spanning Tree status for LtM ports
- LtD status and member ports

## Information dump

**Command:** /info/dump

Use the `dump` command to dump all switch information available from the Information Menu (10K or more, depending on your configuration). This data is useful for tuning and debugging switch performance.

If you want to capture dump data to a file, set the communication software on your workstation to capture session data prior to issuing the dump commands.

# Statistics Menu

## Introduction

You can view switch performance statistics in the user, operator, and administrator command modes. This chapter discusses how to use the CLI to display switch statistics.

## Menu information

**Command:** `/stats`

```
[Statistics Menu]
  port      - Port Stats Menu
  clrports  - Clear stats for all ports
  l2        - Layer 2 Stats Menu
  l3        - Layer 3 Stats Menu
  mp        - MP-specific Stats Menu
  acl       - ACL Stats Menu
  snmp      - Show SNMP stats
  ntp       - Show NTP stats
  ufd       - Show Uplink Failure Detection stats
  sfd       - Show Server Link Failure Detection stats
  clrmpp    - Clear all MP related stats
  dump      - Dump all stats
```

The following table describes the Statistics Menu options.

**Table 44** Statistics Menu options

Command	Usage
<code>port &lt;port number&gt;</code>	Displays the Port Statistics Menu for the specified port. Use this command to display traffic statistics on a port-by-port basis. Traffic statistics are included in SNMP Management Information Base (MIB) objects.
<code>clrports</code>	Clear statistics counters for all ports.
<code>l2</code>	Displays the Layer 2 Statistics Menu.
<code>l3</code>	Displays the Layer 3 Statistics Menu.
<code>mp</code>	Displays the Management Processor Statistics Menu. Use this command to view information on how switch management processes and resources are currently being allocated.
<code>acl</code>	Displays the Access Control List Statistics Menu.
<code>snmp</code>	Displays SNMP statistics.
<code>ntp &lt;clear&gt;</code>	Displays Network Time Protocol (NTP) Statistics. You can execute the clear command option to delete all statistics.
<code>ufd &lt;clear&gt;</code>	Displays Uplink Failure Detection statistics. Add the argument, <code>clear</code> , to clear UFD statistics.



**Table 44** Statistics Menu options

Command	Usage
sfd <clear>	Displays Server Link Failure Detection (SFD) statistics. Add the argument, <code>clear</code> , to clear SFD statistics.
clmp	Clears all Management Processor statistics.
dump	Dumps all switch statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command.

## Port Statistics Menu

**Command:** `/stats/port <port number>`

```
[Port Statistics Menu]
 8021x  - Show 802.1x stats
 brg    - Show bridging ("dot1") stats
 ether  - Show Ethernet ("dot3") stats
 if     - Show interface ("if") stats
 ip     - Show Internet Protocol ("IP") stats
 link   - Show link stats
 rmon   - Show RMON stats
 clear  - Clear all port stats
```

This menu displays traffic statistics on a port-by-port basis.

The following table describes the Port Statistics Menu options:

**Table 45** Port Statistics Menu options

Command	Usage
8021x	Displays IEEE 802.1X statistics
brg	Displays bridging ("dot1") statistics for the port.
ether	Displays Ethernet ("dot3") statistics for the port.
if	Displays interface statistics for the port.
ip	Displays Internet Protocol statistics for the port.
link	Displays link statistics for the port.
rmon	Displays Remote Monitoring (RMON) statistics for the port.
clear	Clears all the statistics on the port.

## 802.1X statistics

**Command:** /stats/port <port number>/8021x

```
Authenticator Statistics:
  eapolFramesRx           = 0
  eapolFramesTx           = 0
  eapolStartFramesRx      = 0
  eapolLogoffFramesRx     = 0
  eapolRespIdFramesRx     = 0
  eapolRespFramesRx       = 0
  eapolReqIdFramesTx      = 0
  eapolReqFramesTx        = 0
  invalidEapolFramesRx    = 0
  eapLengthErrorFramesRx  = 0
  lastEapolFrameVersion   = 0
  lastEapolFrameSource    = 00:00:00:00:00:00

Authenticator Diagnostics:
  authEntersConnecting           = 0
  authEapLogoffsWhileConnecting = 0
  authEntersAuthenticating       = 0
  authSuccessesWhileAuthenticating = 0
  authTimeoutsWhileAuthenticating = 0
  authFailWhileAuthenticating    = 0
  authReauthsWhileAuthenticating = 0
  authEapStartsWhileAuthenticating = 0
  authEapLogoffWhileAuthenticating = 0
  authReauthsWhileAuthenticated = 0
  authEapStartsWhileAuthenticated = 0
  authEapLogoffWhileAuthenticated = 0
  backendResponses                = 0
  backendAccessChallenges         = 0
  backendOtherRequestsToSupplicant = 0
  backendNonNakResponsesFromSupplicant = 0
  backendAuthSuccesses            = 0
  backendAuthFails                = 0
```

The following table describes the 802.1X authenticator diagnostics for a selected port:

**Table 46** 802.1X statistics for port

Statistics	Port
<b>Authenticator Diagnostics</b>	
authEntersConnecting	Total number of times that the state machine transitions to the CONNECTING state from any other state.
authEapLogoffsWhileConnecting	Total number of times that the state machine transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPOL-Logoff message.
authEntersAuthenticating	Total number of times that the state machine transitions from CONNECTING to AUTHENTICATING, as a result of an EAPResponse/ Identity message being received from the Supplicant.
authSuccessesWhileAuthenticating	Total number of times that the state machine transitions from AUTHENTICATING to AUTHENTICATED, as a result of the Backend Authentication state machine indicating successful authentication of the Supplicant.

**Table 46** 802.1X statistics for port

Statistics	Port
authTimeoutsWhileAuthenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of the Backend Authentication state machine indicating authentication timeout.
authFailWhileAuthenticating	Total number of times that the state machine transitions from AUTHENTICATING to HELD, as a result of the Backend Authentication state machine indicating authentication failure.
authReauthsWhileAuthenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of a re-authentication request.
authEapStartsWhileAuthenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Start message being received from the Supplicant.
authEapLogoffWhileAuthenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Logoff message being received from the Supplicant.
authReauthsWhileAuthenticated	Total number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of a re-authentication request.
authEapStartsWhileAuthenticated	Total number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of an EAPOL-Start message being received from the Supplicant.
authEapLogoffWhileAuthenticated	Total number of times that the state machine transitions from AUTHENTICATED to DISCONNECTED, as a result of an EAPOLLogoff message being received from the Supplicant.
backendResponses	Total number of times that the state machine sends an initial Access-Request packet to the Authentication server. Indicates that the Authenticator attempted communication with the Authentication Server.
backendAccessChallenges	Total number of times that the state machine receives an initial Access-Challenge packet from the Authentication server. Indicates that the Authentication Server has communication with the Authenticator.
backendOtherRequestsToSupplicant	Total number of times that the state machine sends an EAP-Request packet (other than an Identity, Notification, Failure, or Success message) to the Supplicant. Indicates that the Authenticator chose an EAP-method.
backendNonNakResponsesFromSupplicant	Total number of times that the state machine receives a response from the Supplicant to an initial EAP-Request, and the response is something other than EAP-NAK. Indicates that the Supplicant can respond to the Authenticators chosen EAP-method.
backendAuthSuccesses	Total number of times that the state machine receives an Accept message from the Authentication Server. Indicates that the Supplicant has successfully authenticated to the Authentication Server.

**Table 46** 802.1X statistics for port

Statistics	Port
backendAuthFails	Total number of times that the state machine receives a Reject message from the Authentication Server. Indicates that the Supplicant has not authenticated to the Authentication Server.

## Bridging statistics

**Command:** `/stats/port <port number>/brg`

```
Bridging statistics for port 1:
dot1PortInFrames:           63242584
dot1PortOutFrames:         63277826
dot1PortInDiscards:         0
dot1TpLearnedEntryDiscards: 0
dot1StpPortForwardTransitions: 0
```

The following table describes the bridging statistics for a selected port:

**Table 47** Bridging statistics for port

Statistics	Description
dot1PortInFrames	The number of frames that have been received by this port from its segment. A frame received on the interface corresponding to this port is counted by this object, if and only if, it is for a protocol being processed by the local bridging function, including bridge management frames.
dot1PortOutFrames	The number of frames that have been transmitted by this port to its segment. A frame transmitted on the interface corresponding to this port is counted by this object, if and only if, it is for a protocol being processed by the local bridging function, including bridge management frames.
dot1PortInDiscards	Count of valid frames received which were discarded (that is, filtered) by the forwarding process.
dot1TpLearnedEntryDiscards	The total number of Forwarding Database entries, which have been or would have been learned, but have been discarded due to a lack of space to store them in the Forwarding Database. If this counter is increasing, it indicates that the Forwarding Database is regularly becoming full (a condition which has adverse performance effects on the sub network). If this counter has a significant value but is not presently increasing, it indicates that the problem has been occurring but is not persistent.
dot1StpPortForwardTransitions	The number of times this port has transitioned from the Learning state to the Forwarding state.

## Ethernet statistics

**Command:** `/stats/port <port number>/ether`

```
Ethernet statistics for port 1:
dot3StatsAlignmentErrors:          0
dot3StatsFCSErrors:                0
dot3StatsSingleCollisionFrames:    0
dot3StatsMultipleCollisionFrames:  0
dot3StatsLateCollisions:           0
dot3StatsExcessiveCollisions:      0
dot3StatsInternalMacTransmitErrors: NA
dot3StatsFrameTooLongs:            0
dot3StatsInternalMacReceiveErrors: 0
```

The following table describes the Ethernet statistics for a selected port:

**Table 48** Ethernet statistics for port

Statistics	Description
<code>dot3StatsAlignmentErrors</code>	<p>A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the Frame Check Sequence (FCS) check.</p> <p>The count represented by an instance of this object is incremented when the <code>AlignmentError</code> status is returned by the MAC service to the Logical Link Control (LLC) (or other MAC user).</p> <p>Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.</p>
<code>dot3StatsFCSErrors</code>	<p>A count of frames received on a particular interface that are an integral number of octets in length but do not pass the Frame Check Sequence (FCS) check.</p> <p>The count represented by an instance of this object is incremented when the <code>frameCheckError</code> status is returned by the MAC service to the LLC (or other MAC user).</p> <p>Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.</p>
<code>dot3StatsSingleCollisionFrames</code>	<p>A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.</p> <p>A frame that is counted by an instance of this object is also counted by the corresponding instance of the <code>ifOutUcastPkts</code>, <code>ifOutMulticastPkts</code>, or <code>ifOutBroadcastPkts</code>, and is not counted by the corresponding instance of the <code>dot3StatsMultipleCollisionFrame</code> object.</p>

**Table 48** Ethernet statistics for port

Statistics	Description
<code>dot3StatsMultipleCollisionFrames</code>	<p>A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.</p> <p>A frame that is counted by an instance of this object is also counted by the corresponding instance of either the <code>ifOutUcastPkts</code>, <code>ifOutMulticastPkts</code>, or <code>ifOutBroadcastPkts</code>, and is not counted by the corresponding instance of the <code>dot3StatsSingleCollisionFrames</code> object.</p>
<code>dot3StatsLateCollisions</code>	<p>The number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet.</p> <p>Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mbps system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.</p>
<code>dot3StatsExcessiveCollisions</code>	<p>A count of frames for which transmission on a particular interface fails due to excessive collisions.</p>
<code>dot3StatsInternalMacTransmitErrors</code>	<p>A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.</p> <p>A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the <code>dot3StatsLateCollisions</code> object, the <code>dot3StatsExcessiveCollisions</code> object, or the <code>dot3StatsCarrierSenseErrors</code> object.</p> <p>The precise meaning of the count represented by an instance of this object is implementation specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted.</p>
<code>dot3StatsFrameTooLongs</code>	<p>A count of frames received on a particular interface that exceeds the maximum permitted frame size.</p> <p>The count represented by an instance of this object is incremented when the <code>frameTooLong</code> status is returned by the MAC service to the LLC (or other MAC user).</p> <p>Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.</p>

**Table 48** Ethernet statistics for port

Statistics	Description
dot3StatsInternalMacReceiveErrors	<p>A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of the dot3StatsFrameTooLongs object, the dot3StatsAlignmentErrors object, or the dot3StatsFCSErrors object.</p> <p>The precise meaning of the count represented by an instance of this object is implementation specific. In particular, an instance of this object may represent a count of received errors on a particular interface that are not otherwise counted.</p>

## Interface statistics

**Command:** /stats/port <port number>/if

```
Interface statistics for port 1:
                ifHCIn Counters          ifHCOut Counters
Octets:                51697080313          51721056808
UcastPkts:              65356399           65385714
BroadcastPkts:          0                  6516
MulticastPkts:          0                  0
Discards:               0                  0
Errors:                 0                  21187
```

The following table describes the interface (IF) statistics for a selected port:

**Table 49** Interface statistics for port

Statistics	Description
Octets-IfHCIn	The total number of octets received on the interface, including framing characters.
UcastPkts-IfHCIn	The number of packets, delivered by this sublayer to a higher sublayer, which were not addressed to a multicast or broadcast address at this sublayer.
BroadcastPkts-IfHCIn	The number of packets, delivered by this sublayer to a higher sublayer, which were addressed to a broadcast address at this sublayer.
MulticastPkts-IfHCIn	<p>The total number of packets, delivered by this sublayer. These are the packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast address at this sublayer, including those that were discarded or not sent.</p> <p>For a MAC layer protocol, this includes both group and functional addresses.</p>
Discards-IfHCIn	The number of inbound packets which were chosen to be discarded even though no errors were detected to prevent their being delivered to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.

**Table 49** Interface statistics for port

Statistics	Description
Errors-IfHCIn	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.
Octets-IfHCOut	The total number of octets transmitted out of the interface, including framing characters.
UcastPkts-IfHCOut	The total number of packets that higher-level protocols requested to be transmitted, and which were not addressed to a multicast or broadcast address at this sublayer, including those that were discarded or not sent.
BroadcastPkts-IfHCOut	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a broadcast address at this sublayer, including those that were discarded or not sent. This object is a 64-bit version of <code>ifOutBroadcastPkts</code> .
MulticastPkts-IfHCOut	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast address at this sublayer, including those that were discarded or not sent. For a MAC layer protocol, this includes both group and functional addresses. This object is a 64-bit version of <code>ifOutMulticastPkts</code> .
Discards-IfHCOut	The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Errors-IfHCOut	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.



## Internet Protocol (IP) statistics

**Command:** `/stats/port <port number>/ip`

```
GEA IP statistics for port 1:
ipInReceives      :      0
ipInHeaderError:    0
ipInDiscards      :      0
```

The following table describes the Internet Protocol (IP) statistics for a selected port:

**Table 50** IP statistics for port

Statistics	Description
ipInReceives	The total number of input datagrams received from interfaces, including those received in error.
ipInHeaderError	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch).
ipInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.

## Link statistics

**Command:** `/stats/port <port number>/link`

```
Link statistics for port 1:
linkStateChange:      2
```

The following table describes the link statistics for a selected port:

**Table 51** Link statistics for port

Statistics	Description
linkStateChange	The total number of link state changes.

## Port RMON statistics

**Command:** `/stats/port <port number>/rmon`

```
RMON statistics for port 2:
etherStatsDropEvents:      NA
etherStatsOctets:          0
etherStatsPkts:            0
etherStatsBroadcastPkts:   0
etherStatsMulticastPkts:   0
etherStatsCRCAlignErrors:  0
etherStatsUndersizePkts:   0
etherStatsOversizePkts:    0
etherStatsFragments:      NA
etherStatsJabbers:         0
etherStatsCollisions:      0
etherStatsPkts64Octets:    0
etherStatsPkts65to127Octets: 0
etherStatsPkts128to255Octets: 0
etherStatsPkts256to511Octets: 0
etherStatsPkts64Octets:    0
etherStatsPkts1024to1518Octets: 0
```

The following table describes the Remote Monitoring (RMON) statistics of the selected port:

**Table 52** RMON statistics

Statistics	Description
etherStatsDropEvents	The total number of packets received that were dropped because of system resource constraints.
etherStatsOctets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
etherStatsPkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
etherStatsBroadcastPkts	The total number of good packets received that were directed to the broadcast address.
etherStatsMulticastPkts	The total number of good packets received that were directed to a multicast address.
etherStatsCRCAlignErrors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
etherStatsUndersizePkts	The total number of packets received that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
etherStatsOversizePkts	The total number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed.

**Table 52** RMON statistics

Statistics	Description
etherStatsFragments	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
etherStatsJabbers	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Jabber is defined as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
etherStatsCollisions	The best estimate of the total number of collisions on this Ethernet segment.
etherStatsPkts64Octets	The total number of packets (including bad packets) received that were less than or equal to 64 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts65to127Octets	The total number of packets (including bad packets) received that were greater than 64 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts128to255Octets	The total number of packets (including bad packets) received that were greater than 127 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts256to511Octets	The total number of packets (including bad packets) received that were greater than 255 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts512to1023Octets	The total number of packets (including bad packets) received that were greater than 511 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts1024to1518Octets	The total number of packets (including bad packets) received that were greater than 1023 octets in length (excluding framing bits but including FCS octets).

## Layer 2 statistics

**Command:** /stats/l2

```
[Layer 2 Statistics Menu]
fdb      - Show FDB stats
lACP     - Show LACP stats
hotlink  - Show Hot Links stats
```

The following table describes the Layer 2 Statistics Menu options.

**Table 53** Layer 2 Statistics Menu options

Command	Usage
fdb	Displays the Forwarding Database statistics menu.
lACP	Displays the Link Aggregation Control Protocol statistics menu.
hotlink	Displays Hot Links statistics.

## FDB statistics

**Command:** /stats/l2/fdb

```
FDB statistics:
current:          91  hiwat:          91
```

This menu option enables you to display statistics regarding the use of the forwarding database, including the number of current entries and the maximum number of entries ever recorded.

The following table describes the Forwarding Database (FDB) statistics:

**Table 54** Forwarding Database statistics

Statistics	Description
current	Current number of entries in the Forwarding Database.
hiwat	Highest number of entries recorded at any given time in the Forwarding Database.

## LACP statistics

**Command:** /stats/l2/lACP <port number>

```
Valid LACPDUs received      - 0
Valid Marker PDUs received  - 0
Valid Marker Rsp PDUs received - 0
Unknown version/TLV type    - 0
Illegal subtype received    - 0
LACPDUs transmitted         - 0
Marker PDUs transmitted     - 0
Marker Rsp PDUs transmitted - 0
```

## Hot Links statistics

**Command:** /stats/l2/hotlink

```
Trigger 1 statistics:
  Trigger Name:  Trigger 1
  Master active:                                0
  Backup active:                                0
  FDB update:  0  failed:                                0
```

The following table describes the Hot Links statistics:

**Table 55** Hot Links statistics

Statistic	Description
Master active	Total number of times the Master interface transitioned to the Active state.
Backup active	Total number of times the Backup interface transitioned to the Active state.
FDB update	Total number of FDB update requests sent.
failed	Total number of FDB update requests that failed.

# Layer 3 statistics

**Command:** /stats/l3

```
[Layer 3 Statistics Menu]
  geal3    - GEA Layer 3 Stats Menu
  ip       - Show IP stats
  route    - Show route stats
  arp      - Show ARP stats
  dns      - Show DNS stats
  icmp     - Show ICMP stats
  tcp      - Show TCP stats
  udp      - Show UDP stats
  igmp     - Show IGMP stats
  ospf     - OSPF stats
  vrrp     - Show VRRP stats
  clrvrrp  - Clear VRRP stats
  rip      - Show RIP stats
  igmpgrps - Total number of IGMP groups
  ipmcgrps - Total number of IPMC groups
  clrigmp  - Clear IGMP stats
  ipclear  - Clear IP stats
  ripclear - Clear RIP stats
  ospfclear - Clear all OSPF stats
  dump     - Dump layer 3 stats
```

The following table describes the Layer 3 Statistics Menu options.

**Table 56** Layer 3 Statistics Menu options

Command	Usage
geal3	Displays the GEA statistics menu.
ip	Displays IP statistics.
route	Displays route statistics.
arp <clear>	Displays Address Resolution Protocol (ARP) statistics. Add the argument <code>clear</code> , to clear ARP statistics.
dns	Displays Domain Name System (DNS) statistics.
icmp	Displays ICMP statistics.
tcp	Displays Transmission Control Protocol (TCP) statistics. Add the argument, <code>clear</code> , to clear TCP statistics.
udp	Displays User Datagram Protocol (UDP) statistics. Add the argument, <code>clear</code> , to clear UDP statistics.
igmp	Displays IGMP statistics.
ospf	Displays OSPF statistics menu.
vrrp	When virtual routers are configured, you can display statistics for the virtual routers.
clrvrrp	Clears VRRP statistics.
rip	Displays Routing Information Protocol (RIP) statistics.
igmpgrps	Displays the total number of Internet Group Management Protocol (IGMP) groups registered the switch.

**Table 56** Layer 3 Statistics Menu options

Command	Usage
ipmcgrps	Displays the total number of Internet Protocol Multicast (IPMC) groups registered on the switch.
clrigmp <1-4094> all	Clears all IGMP statistics for the selected VLANs.
ipclear	Clears IP statistics. Use this command with caution as it will delete all the IP statistics.
ripclear	Clears all Routing Information Protocol (RIP) statistics.
ospfclear	Clears all Open Shortest Path First (OSPF) statistics.
dump	Displays all Layer 3 statistics.

## GEA Layer 3 statistics menu

**Command:** /stats/l3/geal3

```
[GEA Layer 3 Statistics Menu]
  l3bucket - Show GEA L3 bucket for an IP address
  dump     - Dump GEA layer 3 stats counter
```

The following table describes the Layer 3 GEA Statistics Menu options.

**Table 57** Layer 3 GEA statistics menu options

Command	Usage
l3bucket	Displays GEA statistics for a specific IP address.
Dump	Displays all GEA statistics.

## GEA statistics

**Command:** /stats/l3/geal3/dump

```
GEA L3 statistics:
  Max L3 table size           : 4096
  Number of L3 entries used   : 3

  Max LPM table size          : 512
  Number of LPM entries used   : 4
```

## IP statistics

**Command:** /stats/l3/ip

```
IP statistics:
ipInReceives: 36475          ipInHdrErrors: 0
ipInAddrErrors: 905
ipInUnknownProtos: 0        ipInDiscards: 0
ipInDelivers: 4103          ipOutRequests: 30974
ipOutDiscards: 0
ipDefaultTTL: 255
```

The following table describes the IP statistics:

**Table 58** IP statistics

Statistics	Description
ipInReceives	The total number of input datagrams received from interfaces, including those received in error.
ipInHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on.
ipInAddrErrors	The number of input datagrams discarded because the IP address in their IP header destination field was not a valid address to be received at this switch. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported classes (for example, Class E). For entities which are not IP gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
ipInUnknownProtos	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
ipInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). This counter does not include any datagrams discarded while awaiting re-assembly.
ipInDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
ipOutRequests	The total number of IP datagrams that local IP user-protocols (including ICMP) supplied to IP in requests for transmission. This counter does not include any datagrams counted in ipForwDatagrams.
ipOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space). This counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
ipDefaultTTL	The default value inserted into the Time-To-Live (TTL) field of the IP header of datagrams originated at this switch, whenever a TTL value is not supplied by the transport layer protocol.



## Route statistics

**Command:** /stats/l3/route

```
Route statistics:
ipRoutesCur:      8   ipRoutesHighWater:      8
ipRoutesMax:     4096
```

The following table describes the Route statistics:

**Table 59** Route statistics

Statistics	Description
ipRoutesCur	The total number of outstanding routes in the route table.
ipRoutesMax	The maximum number of supported routes.
ipRoutesHighWater	The highest number of routes ever recorded in the route table.

## ARP statistics

**Command:** /stats/l3/arp

```
ARP statistics:
arpEntriesCur:      2   arpEntriesHighWater:      4
arpEntriesMax:     4095
```

The following table describes the Address Resolution Protocol (ARP) statistics:

**Table 60** ARP statistics

Statistics	Description
arpEntriesCur	The total number of outstanding ARP entries in the ARP table.
arpEntriesMax	The maximum number of ARP entries that are supported.
arpEntriesHighWater	The highest number of ARP entries ever recorded in the ARP table.

## DNS statistics

**Command:** /stats/l3/dns

```
DNS statistics:
dnsInRequests:      0   dnsOutRequests:      0
dnsBadRequests:      0
```

The following table describes the Domain Name System (DNS) statistics:

**Table 61** DNS statistics

Statistics	Description
dnsInRequests	The total number of DNS request packets that have been received.
dnsOutRequests	The total number of DNS response packets that have been transmitted.
dnsBadRequests	The total number of DNS request packets received that were dropped.

## ICMP statistics

**Command:** `/stats/l3/icmp`

```

ICMP statistics:
icmpInMsgs:                245802    icmpInErrors:                1393
icmpInDestUnreaches:       41        icmpInTimeExcds:             0
icmpInParmProbs:           0         icmpInSrcQuenchs:            0
icmpInRedirects:           0         icmpInEchos:                 18
icmpInEchoReps:            244350    icmpInTimestamps:           0
icmpInTimestampReps:       0         icmpInAddrMasks:             0
icmpInAddrMaskReps:        0         icmpOutMsgs:                 253810
icmpOutErrors:             0         icmpOutDestUnreaches:        15
icmpOutTimeExcds:          0         icmpOutParmProbs:            0
icmpOutSrcQuenchs:         0         icmpOutRedirects:            0
icmpOutEchos:              253777    icmpOutEchoReps:            18
icmpOutTimestamps:         0         icmpOutTimestampReps:        0
icmpOutAddrMasks:         0         icmpOutAddrMaskReps:         0
  
```

The following table describes the Internet Control Messaging Protocol (ICMP) statistics:

**Table 62** ICMP statistics

Statistics	Description
icmpInMsgs	The total number of ICMP messages which the switch received. Note that this counter includes all those counted by icmpInErrors.
icmpInErrors	The number of ICMP messages which the switch received but determined as having ICMP specific errors (for example bad ICMP checksums and bad length).
icmpInDestUnreaches	The number of ICMP Destination Unreachable messages received.
icmpInTimeExcds	The number of ICMP Time Exceeded messages received.
icmpInParmProbs	The number of ICMP Parameter Problem messages received.
icmpInSrcQuenchs	The number of ICMP Source Quench (buffer almost full, stop sending data) messages received.
icmpInRedirects	The number of ICMP Redirect messages received.
icmpInEchos	The number of ICMP Echo (request) messages received.
icmpInEchoReps	The number of ICMP Echo Reply messages received.
icmpInTimestamps	The number of ICMP Timestamp (request) messages received.
icmpInTimestampReps	The number of ICMP Timestamp Reply messages received.
icmpInAddrMasks	The number of ICMP Address Mask Request messages received.
icmpInAddrMaskReps	The number of ICMP Address Mask Reply messages received.
icmpOutMsgs	The total number of ICMP messages which this switch attempted to send. Note that this counter includes all those counted by icmpOutErrors.
icmpOutErrors	The number of ICMP messages that this switch did not send due to problems discovered within ICMP such as a lack of buffer. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of errors that contribute to this counter's value.

**Table 62** ICMP statistics

Statistics	Description
icmpOutDestUnreachs	The number of ICMP Destination Unreachable messages sent.
icmpOutTimeExcds	The number of ICMP Time Exceeded messages sent.
icmpOutParmProbs	The number of ICMP Parameter Problem messages sent.
icmpOutSrcQuenchs	The number of ICMP Source Quench (buffer almost full, stop sending data) messages sent.
icmpOutRedirects	The number of ICMP Redirect messages sent.
icmpOutEchos	The number of ICMP Echo (request) messages sent.
icmpOutEchoReps	The number of ICMP Echo Reply messages sent.
icmpOutTimestamps	The number of ICMP Timestamp (request) messages sent.
icmpOutTimestampReps	The number of ICMP Timestamp Reply messages sent.
icmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.
icmpOutAddrMaskReps	The number of ICMP Address Mask Reply messages sent.

## TCP statistics

**Command:** /stats/l3/tcp

```

TCP statistics:
tcpRtoAlgorithm:      4      tcpRtoMin:      0
tcpRtoMax:           240000  tcpMaxConn:     512
tcpActiveOpens:      252214  tcpPassiveOpens: 7
tcpAttemptFails:      528    tcpEstabResets:  4
tcpInSegs:           756401  tcpOutSegs:      756655
tcpRetransSegs:       0      tcpInErrs:       0
tcpCurBuff:          0      tcpCurConn:     3
tcpOutRsts:           417

```

The following table describes the Transmission Control Protocol (TCP) statistics:

**Table 63** TCP statistics

Statistics	Description
tcpRtoAlgorithm	The algorithm used to determine the timeout value used for retransmitting unacknowledged octets.
tcpRtoMin	The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the LBOUND quantity described in Request For Comments (RFC) 793.

**Table 63** TCP statistics

Statistics	Description
<code>tcpRtoMax</code>	The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is <code>rsre(3)</code> , an object of this type has the semantics of the <code>UBOUND</code> quantity described in RFC 793.
<code>tcpMaxConn</code>	The limit on the total number of TCP connections the switch can support. In entities where the maximum number of connections is dynamic, this object should contain the value <code>-1</code> .
<code>tcpActiveOpens</code>	The number of times TCP connections have made a direct transition to the <code>SYN-SENT</code> state from the <code>CLOSED</code> state.
<code>tcpPassiveOpens</code>	The number of times TCP connections have made a direct transition to the <code>SYN-RCVD</code> state from the <code>LISTEN</code> state.
<code>tcpAttemptFails</code>	The number of times TCP connections have made a direct transition to the <code>CLOSED</code> state from either the <code>SYN-SENT</code> state or the <code>SYN-RCVD</code> state, plus the number of times TCP connections have made a direct transition to the <code>LISTEN</code> state from the <code>SYN-RCVD</code> state.
<code>tcpEstabResets</code>	The number of times TCP connections have made a direct transition to the <code>CLOSED</code> state from either the <code>ESTABLISHED</code> state or the <code>CLOSE-WAIT</code> state.
<code>tcpInSegs</code>	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
<code>tcpOutSegs</code>	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
<code>tcpRetransSegs</code>	The total number of segments retransmitted, that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
<code>tcpInErrs</code>	The total number of segments received in error (for example, bad TCP checksums).
<code>tcpCurBuff</code>	The total number of outstanding memory allocations from heap by TCP protocol stack.
<code>tcpCurConn</code>	The total number of outstanding TCP sessions that are currently opened.
<code>tcpOutRsts</code>	The number of TCP segments sent containing the reset (RST) flag.

## UDP statistics

**Command:** `/stats/l3/udp`

```
UDP statistics:
udpInDatagrams:      54    udpOutDatagrams:      43
udpInErrors:         0    udpNoPorts:      1578077
```

The following table describes the User Datagram Protocol (UDP) statistics:

**Table 64** UDP statistics

Statistics	Description
udpInDatagrams	The total number of UDP datagrams delivered to the switch.
udpOutDatagrams	The total number of UDP datagrams sent from this switch.
udpInErrors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
udpNoPorts	The total number of received UDP datagrams for which there was no application at the destination port.

## IGMP Multicast Group statistics

**Command:** `/stats/l3/igmp <VLAN number>`

```
-----
IGMP Snoop vlan 1 statistics:
-----
rxIgmpValidPkts:      0    rxIgmpInvalidPkts:      0
rxIgmpGenQueries:     0    rxIgmpGrpSpecificQueries:  0
rxIgmpGroupSrcSpecificQueries: 0
rxIgmpLeaves:         0    rxIgmpReports:          0
txIgmpReports:        0    txIgmpGrpSpecificQueries:  0
txIgmpLeaves:         0    rxIgmpV3CurrentStateRecords: 0
rxIgmpV3SourceListChangeRecords: 0    rxIgmpV3FilterChangeRecords: 0
```

This menu option enables you to display statistics regarding the use of the IGMP Multicast Groups.

The following table describes the IGMP statistics:

**Table 65** IGMP statistics

Statistic	Description
rxIgmpValidPkts	Total number of valid IGMP packets received
rxIgmpInvalidPkts	Total number of invalid packets received
rxIgmpGenQueries	Total number of General Membership Query packets received
rxIgmpGrpSpecificQueries	Total number of Membership Query packets received from specific groups
rxIgmpGroupSrcSpecificQueries	Total number of Group Source-Specific Queries (GSSQ) received
rxIgmpLeaves	Total number of Leave requests received

**Table 65** IGMP statistics

Statistic	Description
rxIgmpReports	Total number of Membership Reports received
txIgmpReports	Total number of Membership reports transmitted
txIgmpGrpSpecificQueries	Total number of Membership Query packets transmitted to specific groups
txIgmpLeaves	Total number of Leave messages transmitted
rxIgmpV3CurrentStateRecords	Total number of Current State records received
rxIgmpV3SourceListChangeRecords	Total number of Source List Change records received
rxIgmpV3FilterChangeRecords	Total number of Filter Change records received.

## OSPF statistics menu

**Command:** /stats/l3/ospf

```
[OSPF stats Menu]
  general - Show global stats
  aindex  - Show area(s) stats
  if      - Show interface(s) stats
```

The following table describes the OSPF statistics menu options.

**Table 66** OSPF statistics menu options

Command	Usage
general	Displays OSPF global statistics.
aindex <0-2>	Displays area index statistics.
if <1-249>	Displays interface statistics.

## OSPF global statistics

**Command:** /stats/l3/ospf/general

```

OSPF stats
-----
Rx/Tx Stats:                Rx                Tx
-----
Pkts                        0                0
hello                      23             518
database                    4             12
ls requests                 3              1
ls acks                     7              7
ls updates                  9              7
Nbr change stats:          Intf change Stats:
hello                      2             up 4
start                      0             down 2
n2way                      2             loop 0
adjoint ok                 2             unloop 0
negotiation done           2             wait timer 2
exchange done              2             backup 0
bad requests               0             nbr change 5
bad sequence               0
loading done               2
nlway                      0
rst_ad                     0
down                       1
Timers kickoff
hello                      514
retransmit                1028
lsa lock                   0
lsa ack                    0
dbage                      0
summary                   0
ase export                 0
  
```

The following table describes the OSPF global statistics:

**Table 67** OSPF global statistics

Statistic	Description
Rx Tx stats:	
Rx Pkts	The sum total of all OSPF packets received on all OSPF areas and interfaces.
Tx Pkts	The sum total of all OSPF packets transmitted on all OSPF areas and interfaces.
Rx Hello	The sum total of all Hello packets received on all OSPF areas and interfaces.
Tx Hello	The sum total of all Hello packets transmitted on all OSPF areas and interfaces.
Rx Database	The sum total of all Database Description packets received on all OSPF areas and interfaces.
Tx Database	The sum total of all Database Description packets transmitted on all OSPF areas and interfaces.
Rx ls Requests	The sum total of all Link State Request packets received on all OSPF areas and interfaces.
Tx ls Requests	The sum total of all Link State Request packets transmitted on all OSPF areas and interfaces.

**Table 67** OSPF global statistics

Statistic	Description
Rx ls Acks	The sum total of all Link State Acknowledgement packets received on all OSPF areas and interfaces.
Tx ls Acks	The sum total of all Link State Acknowledgement packets transmitted on all OSPF areas and interfaces.
Rx ls Updates	The sum total of all Link State Update packets received on all OSPF areas and interfaces.
Tx ls Updates	The sum total of all Link State Update packets transmitted on all OSPF areas and interfaces.
Nbr change stats:	
hello	The sum total of all Hello packets received from neighbors on all OSPF areas and interfaces.
Start	The sum total number of neighbors in this state (that is, an indication that Hello packets should now be sent to the neighbor at intervals of HelloInterval seconds) across all OSPF areas and interfaces.
n2way	The sum total number of bidirectional communication establishment between this router and other neighboring routers.
adjoint ok	The sum total number of decisions to be made (again) as to whether an adjacency should be established/maintained with the neighbor across all OSPF areas and interfaces.
negotiation done	The sum total number of neighbors in this state wherein the Master/slave relationship has been negotiated, and sequence numbers have been exchanged, across all OSPF areas and interfaces.
exchange done	The sum total number of neighbors in this state (that is, in an adjacency's final state) having transmitted a full sequence of Database Description packets, across all OSPF areas and interfaces.
bad requests	The sum total number of Link State Requests which have been received for a link state advertisement not contained in the database across all interfaces and OSPF areas.
bad sequence	<p>The sum total number of Database Description packets which have been received that either:</p> <ul style="list-style-type: none"> <li>• Has an unexpected DD sequence number</li> <li>• Unexpectedly has the init bit set</li> <li>• Has an options field differing from the last Options field received in a Database Description packet.</li> </ul> <p>Any of these conditions indicate that some error has occurred during adjacency establishment for all OSPF areas and interfaces.</p>
loading done	The sum total number of link state updates received for all out-of-date portions of the database across all OSPF areas and interfaces.
nlway	The sum total number of Hello packets received from neighbors, in which this router is not mentioned across all OSPF interfaces and areas.
rst_ad	The sum total number of times the Neighbor adjacency has been reset across all OSPF areas and interfaces.



**Table 67** OSPF global statistics

Statistic	Description
down	The total number of Neighboring routers down (that is, in the initial state of a neighbor conversation) across all OSPF areas and interfaces.
Intf Change Stats:	
up	The sum total number of interfaces up in all OSPF areas.
down	The sum total number of interfaces down in all OSPF areas.
loop	The sum total of interfaces no longer connected to the attached network across all OSPF areas and interfaces.
unloop	The sum total number of interfaces, connected to the attached network in all OSPF areas.
wait timer	The sum total number of times the Wait Timer has been fired, indicating the end of the waiting period that is required before electing a (Backup) Designated Router across all OSPF areas and interfaces.
backup	The sum total number of Backup Designated Routers on the attached network for all OSPF areas and interfaces.
nbr change	The sum total number of changes in the set of bidirectional neighbors associated with any interface across all OSPF areas.
Timers Kickoff:	
hello	The sum total number of times the Hello timer has been fired (which triggers the send of a Hello packet) across all OPSF areas and interfaces.
retransmit	The sum total number of times the Retransmit timer has been fired across all OPSF areas and interfaces.
lsa lock	The sum total number of times the Link State Advertisement (LSA) lock timer has been fired across all OSPF areas and interfaces.
lsa ack	The sum total number of times the LSA Ack timer has been fired across all OSPF areas and interfaces.
dbage	The total number of times the data base age (Dbage) has been fired.
summary	The total number of times the Summary timer has been fired.
ase export	The total number of times the Autonomous System Export (ASE) timer has been fired.

## VRRP statistics

Virtual Router Redundancy Protocol (VRRP) support on the HP 10GbE switch provides redundancy between routers in a LAN. This is accomplished by configuring the same virtual router IP address and ID number on each participating VRRP-capable routing device.

One of the virtual routers is then elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will assume routing authority and take control of the virtual router IP address.

When virtual routers are configured, you can display protocol statistics for VRRP.

**Command:** `/stats/l3/vrrp`

```
>> Layer 3 Statistics# vrrp
VRRP statistics:
vrrpInAdvers:          0    vrrpBadAdvers:          0
vrrpOutAdvers:          0
vrrpBadVersion:         0    vrrpBadVrid:          0
vrrpBadAddress:         0    vrrpBadData:          0
vrrpBadPassword:        0    vrrpBadInterval:      0
```

The following table describes the VRRP statistics.

**Table 68** VRRP statistics

Field	Description
vrrpInAdvers	The total number of VRRP advertisements that have been received.
vrrpOutAdvers	The total number of VRRP advertisements that have been sent.
vrrpBadVersion	The total number of VRRP advertisements that had a bad version number.
vrrpBadAddress	The total number of VRRP advertisements that had a bad address.
vrrpBadPassword	The total number of VRRP advertisements that had a bad password.
vrrpBadAdvers	The total number of VRRP advertisements received that were dropped.
vrrpBadVrid	The total number of VRRP advertisements that had a bad virtual router ID.
vrrpBadData	The total number of VRRP advertisements that had bad data.
vrrpBadInterval	The total number of VRRP advertisements that had a bad interval.

## RIP statistics

**Command:** /stats/l3/rip

```
RIP ALL STATS INFORMATION:  
  RIP packets received = 12  
  RIP packets sent = 75  
  RIP request received = 0  
  RIP response received = 12  
  RIP request sent = 3  
  RIP response sent = 72  
  RIP route timeout = 0  
  RIP bad size packet received = 0  
  RIP bad version received = 0  
  RIP bad zeros received = 0  
  RIP bad src port received = 0  
  RIP bad src IP received = 0  
  RIP packets from self received = 0
```

# Management Processor statistics

**Command:** /stats/mp

```
[MP-specific Statistics Menu]
  pkt      - Show Packet stats
  tcb      - Show All TCP control blocks in use
  ucb      - Show All UDP control blocks in use
  cpu      - Show CPU utilization
```

The following table describes the Statistics Menu options for the management processor (MP):

**Table 69** MP-specific Statistics Menu options

Command	Usage
pkt	Displays packet statistics, to check for leads and load.
tcb	Displays all Transmission Control Protocol (TCP) control blocks (TCB) that are in use.
ucb	Displays all User Datagram Protocol (UDP) control blocks (UCB) that are in use.
cpu	Displays CPU utilization for periods of up to 1, 4, and 64 seconds.

## Packet statistics

**Command:** /stats/mp/pkt

```
Packet counts:
allocs:          36692      frees:          36692
mediums:          0      mediums hi-watermark:    3
jumbos:          0      jumbos hi-watermark:    0
smalls:          0      smalls hi-watermark:    2
failures:         0
```

The following table describes the packet statistics.

**Table 70** MP specific packet statistics

Description	Example statistic
allocs	Total number of packet allocations from the packet buffer pool by the TCP/IP protocol stack.
frees	Total number of times the packet buffers are freed (released) to the packet buffer pool by the TCP/IP protocol stack.
mediums	Total number of packet allocations with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
mediums hi-watermark	The highest number of packet allocation with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
jumbos	Total number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
jumbos hi-watermark	The highest number of packet allocation with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
smalls	Total number of packet allocations with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.

**Table 70** MP specific packet statistics

Description	Example statistic
smalls hi-watermark	The highest number of packet allocation with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
failures	Total number of packet allocation failures from the packet buffer pool by the TCP/IP protocol stack.

## TCP statistics

**Command:** `/stats/mp/tcb`

```
All TCP allocated control blocks:
10ad41e8:  0.0.0.0          0 <=> 0.0.0.0          80  listen
10ad5790:  47.81.27.5         1171 <=> 47.80.23.243    23  established
```

The following table describes the Transmission Control Protocol (TCP) control block (TCB) statistics shown in this example:

**Table 71** TCP statistics

Description	Example statistic
Memory	10ad41e8/10ad5790
Destination IP address	0.0.0.0/47.81.27.5
Destination port	0/1171
Source IP	0.0.0.0/47.80.23.243
Source port	80/23
State	listen/established

## UDP statistics

**Command:** `/stats/mp/ucb`

```
All UDP allocated control blocks:
161:  listen
```

The following table describes the User Datagram Protocol (UDP) control block (UCB) statistics shown in this example:

**Table 72** UDP statistics

Description	Example Statistic
Control block	161
State	listen

## CPU statistics

**Command:** `/stats/mp/cpu`

```
CPU utilization:
cpuUtil1Second:      8%
cpuUtil4Seconds:     9%
cpuUtil64Seconds:    8%
```

The following table describes the management port CPU utilization statistics:

**Table 73** CPU statistics

Statistics	Description
cpuUtil1Second	The utilization of MP CPU over 1 second. This is shown as a percentage.
cpuUtil4Seconds	The utilization of MP CPU over 4 seconds. This is shown as a percentage.
cpuUtil64Seconds	The utilization of MP CPU over 64 seconds. This is shown as a percentage.

## Access Control List (ACL) statistics menu

**Command:** `/stats/acl`

```
[ACL Menu]
acl      - Display ACL stats
dump     - Display all available ACL stats
clracl   - Clear ACL stats
```

The following table describes the Access Control List (ACL) Statistics menu options:

**Table 74** ACL statistics menu options

Command	Usage
acl <1-384>	Displays the Access Control List Statistics for a specific ACL.
dump	Displays all ACL statistics.
clracl	Clear all ACL statistics.

## ACL statistics

**Command:** `/stats/acl/dump`

```
Hits for ACL 1: 26057515
Hits for ACL 2: 26057497
```

# SNMP statistics

**Command:** /stats/snmp

```
SNMP statistics:
snmpInPkts:          54    snmpInBadVersions:      0
snmpInBadC'tyNames:  0    snmpInBadC'tyUses:      0
snmpInASNParseErrs:  0    snmpEnableAuthTraps:    0
snmpOutPkts:         54    snmpInBadTypes:         0
snmpInTooBig:        0    snmpInNoSuchNames:      0
snmpInBadValues:     0    snmpInReadOnly:         0
snmpInGenErrs:       0    snmpInTotalReqVars:     105
snmpInTotalSetVars:  0    snmpInGetRequests:      2
snmpInGetNexts:      52    snmpInSetRequests:      0
snmpInGetResponses:  0    snmpInTraps:            0
snmpOutTooBig:       0    snmpOutNoSuchNames:     2
snmpOutBadValues:    0    snmpOutReadOnly:        0
snmpOutGenErrs:      0    snmpOutGetRequests:     0
snmpOutGetNexts:     0    snmpOutSetRequests:     0
snmpOutGetResponses: 54    snmpOutTraps:           0
snmpSilentDrops:     0    snmpProxyDrops:         0
```

The following table describes the Simple Network Management Protocol (SNMP) statistics:

**Table 75** SNMP statistics

Statistics	Description
snmpInPkts	The total number of messages delivered to the SNMP entity from the transport service.
snmpInBadVersions	The total number of SNMP messages, which were delivered to the SNMP protocol entity and were for an unsupported SNMP version.
snmpInBadC'tyNames	The total number of SNMP messages delivered to the SNMP entity that used an SNMP community name not known to the switch.
snmpInBadC'tyUses	The total number of SNMP messages delivered to the SNMP protocol entity that represented an SNMP operation which was not allowed by the SNMP community named in the message.
snmpInASNParseErrs	<p>The total number of ASN.1 (Abstract Syntax Notation One) or BER (Basic Encoding Rules), errors encountered by the SNMP protocol entity when decoding SNMP messages received.</p> <p>The Open Systems Interconnection (OSI) method of specifying abstract objects is called ASN.1 (Abstract Syntax Notation One, defined in X.208), and one set of rules for representing such objects as strings of ones and zeros is called the BER (Basic Encoding Rules, defined in X.209).</p> <p>ASN.1 is a flexible notation that allows one to define a variety of data types, from simple types such as integers and bit strings to structured types such as sets and sequences.</p> <p>BER describes how to represent or encode values of each ASN.1 type as a string of eight-bit octets.</p>
snmpEnableAuthTraps	An object to enable or disable the authentication traps generated by this switch.
snmpOutPkts	The total number of SNMP messages which were passed from the SNMP protocol entity to the transport service.
snmpInBadTypes	The total number of SNMP messages which failed ASN.1 parsing.

**Table 75** SNMP statistics

Statistics	Description
snmpInTooBigs	The total number of SNMP Protocol Data Units (PDUs) that were delivered to the SNMP protocol entity and for which the value of the error-status field is too big.
snmpInNoSuchNames	The total number of SNMP Protocol Data Units (PDUs) that were delivered to the SNMP protocol entity and for which the value of the error-status field is noSuchName.
snmpInBadValues	The total number of SNMP Protocol Data Units (PDUs) that were delivered to the SNMP protocol entity and for which the value of the error-status field is badValue.
snmpInReadOnlys	<p>The total number of valid SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is read-only.</p> <p>It should be noted that it is a protocol error to generate an SNMP PDU, which contains the value read-only in the error-status field. As such, this object is provided as a means of detecting incorrect implementations of the SNMP.</p>
snmpInGenErrs	The total number of SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is genErr.
snmpInTotalReqVars	The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as a result of receiving valid SNMP Get-Request and Get-Next Protocol Data Units (PDUs).
snmpInTotalSetVars	The total number of MIB objects, which have been altered successfully by the SNMP protocol entity as a result of receiving valid SNMP Set-Request Protocol Data Units (PDUs).
snmpInGetRequests	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInGetNexts	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInSetRequests	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInGetResponses	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInTraps	The total number of SNMP Trap Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpOutTooBigs	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is too big.
snmpOutNoSuchNames	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status is noSuchName.
snmpOutBadValues	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is badValue.
snmpOutReadOnlys	Not in use.
snmpOutGenErrs	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is genErr.



**Table 75** SNMP statistics

Statistics	Description
snmpOutGetRequests	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutGetNexts	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutSetRequests	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutGetResponses	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutTraps	The total number of SNMP Trap Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpSilentDrops	The total number of GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs delivered to the SNMP entity which were silently dropped because the size of a reply containing an alternate Response-PDU with an empty variable-bindings field was too large.
snmpProxyDrops	The total number of GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs delivered to the SNMP entity that were silently dropped because the transmission of the message to a proxy target failed in a manner (other than a time-out) such that no Response-PDU could be returned.

## NTP statistics

**Command:** /stats/ntp

```
NTP statistics:
  Primary Server:
    Requests Sent:          17
    Responses Received:     17
    Updates:                1
  Secondary Server:
    Requests Sent:          0
    Responses Received:     0
    Updates:                0
```

The switch uses NTP (Network Timing Protocol) version 3 to synchronize the switch's internal clock with an atomic time-calibrated NTP server. With NTP enabled, the switch can accurately update its internal clock to be consistent with other devices on the network and generates accurate syslogs.

The following table describes the NTP statistics:

**Table 76** NTP statistics

Statistics	Description
Primary Server	<ul style="list-style-type: none"><li>• <b>Requests Sent</b>—The total number of NTP requests the switch sent to the primary NTP server to synchronize time.</li><li>• <b>Responses Received</b>—The total number of NTP responses received from the primary NTP server.</li><li>• <b>Updates</b>—The total number of times the switch updated its time based on the NTP responses received from the primary NTP server.</li></ul>
Secondary Server	<ul style="list-style-type: none"><li>• <b>Requests Sent</b>—The total number of NTP requests the switch sent to the secondary NTP server to synchronize time.</li><li>• <b>Responses Received</b>—The total number of NTP responses received from the secondary NTP server.</li><li>• <b>Updates</b>—The total number of times the switch updated its time based on the NTP responses received from the secondary NTP server.</li></ul>

## Uplink Failure Detection statistics

This menu option allows you to display Uplink Failure Detection (UFD) statistics. To reset UFD statistics, follow the command `/stats/ufd` with the following argument: `clear`.

**Command:** `/stats/ufd`

```
Uplink Failure Detection statistics:
Number of times LtM link failure: 1
Number of times LtM link in Blocking State: 0
Number of times LtD got auto disabled: 1
```

The following table describes the Uplink Failure Detection (UFD) statistics:

**Table 77** Uplink Failure Detection statistics

Statistics	Description
Number of times LtM link failure	The total numbers of times that link failures were detected on the uplink ports in the Link to Monitor group.
Number of times LtM link in Blocking State	The total number of times that Spanning Tree Blocking state was detected on the uplink ports in the Link to Monitor group.
Number of times LtD got auto disabled	The total numbers of times that downlink ports in the Link to Disable group were automatically disabled because of a failure in the Link to Monitor group.

# Statistics dump

**Command:** `/stats/dump`

Use the `dump` command to dump all switch statistics available from the Statistics Menu (40K or more, depending on your configuration). This data can be used to tune or debug switch performance.

If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.

# Configuration Menu

## Introduction

The Configuration Menu is only available from an administrator login. It includes submenus for configuring every aspect of the switch. Changes to configuration are not active until explicitly applied. Changes can be saved to non-volatile memory (NVRAM).

## Menu information

**Command:** /cfg

```
[Configuration Menu]
  sys      - System-wide Parameter Menu
  port     - Port Menu
  l2       - Layer 2 Menu
  l3       - Layer 3 Menu
  qos      - QOS Menu
  acl      - Access Control List Menu
  rmon     - RMON Menu
  pmirr    - Port Mirroring Menu
  ufd      - Uplink Failure Detection Menu
  sfd      - Server Link Failure Detection Menu
  dump     - Dump current configuration to script file
  ptcfg    - Backup current configuration to FTP/TFTP server
  gtcfg    - Restore current configuration from FTP/TFTP server
  cur      - Display current configuration
```

The following table describes the Configuration Menu options.

**Table 78** Configuration Menu options

Command	Usage
sys	Displays the System Configuration Menu.
port <port number>	Displays the Port Configuration Menu.
l2	Displays the Layer 2 Configuration Menu.
l3	Displays the Layer 3 Configuration Menu.
qos	Displays the Quality of Service Configuration Menu.
acl	Displays the Access Control List Configuration Menu.
rmon	Displays the RMON Configuration Menu.
pmirr	Displays the Mirroring Configuration Menu.
ufd	Displays the Uplink Failure Detection Configuration Menu.
sfd	Displays the Server Link Failure Detection Configuration Menu.
dump	Dumps current configuration to a script file.

**Table 78** Configuration Menu options

Command	Usage
<code>ptcfg &lt;host name or IP address of FTP/TFTP server&gt; &lt;filename on host&gt;</code>	Backs up current configuration to FTP/TFTP server.
<code>gtcfg &lt;host name or IP address of FTP/TFTP server&gt; &lt;filename on host&gt;</code>	Restores current configuration from FTP/TFTP server.
<code>cur</code>	Displays the current configuration parameters.

## Viewing, applying, reverting, and saving changes

As you use the configuration menus to set switch parameters, the changes you make do not take effect immediately. All changes are considered pending until you explicitly apply them. Also, any changes are lost the next time the switch boots unless the changes are explicitly saved.

While configuration changes are in the pending state, you can:

- View the pending changes
- Apply the pending changes
- Revert to restore configuration parameters set with the last apply command
- Save the changes to flash memory

## Viewing pending changes

You can view all pending configuration changes by entering `diff` at any CLI prompt:

```
# diff
```

You can view all pending configuration changes that have been applied but not saved to flash memory by entering `diff flash` at any CLI prompt:

```
# diff flash
```

## Applying pending changes

To make your configuration changes active, you must apply them. To apply configuration changes, enter the following command at any prompt:

```
# apply
```

**NOTE:** All configuration changes take effect immediately when applied.

## Reverting changes

The `revert` command removes configuration changes that have been made, but not applied. Enter `revert apply` to remove all changes that have not been saved:

```
# revert
```

# Saving the configuration

In addition to applying the configuration changes, you can save them to flash memory on the switch.



**IMPORTANT:** If you do not save the changes, they will be lost the next time the system is rebooted.

To save the new configuration, enter the following command at any prompt:

```
# save
```

When you save configuration changes, the changes are saved to the active configuration block. The configuration being replaced by the save is first copied to the backup configuration block. If you do not want the previous configuration block copied to the backup configuration block, enter the following instead:

```
# save n
```

You can decide which configuration you want to run the next time you reset the switch. Your options include:

- The active configuration block
- The backup configuration block
- Factory default configuration block

You can view all pending configuration changes that have been applied but not saved to flash memory using the `diff flash` command. It is a global command that can be executed from any prompt.

For instructions on selecting the configuration to run at the next system reset, see the “Selecting a configuration block” section in the “Boot Options Menu” chapter.

## Reminders

CLI reminders prompt users to complete configuration tasks that require multiple steps. The default setting for CLI reminders is enabled. Use the following command to disable CLI reminders:

```
/cfg/sys/reminders dis
```

The following is an example of a configuration task performed with CLI reminders enabled.

```
>> Layer 2# vlan 5
VLAN number 5 with name "VLAN 5" created.
Reminder: VLAN 5 needs to be enabled.
>> VLAN 5# add 9
Port 9 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 5 [y/n]: y
Current ports for VLAN 5:          empty
Pending new ports for VLAN 5:      9
Reminder: Port 9 needs to be enabled.
Reminder: VLAN 5 needs to be enabled.
```

# System configuration

**Command:** /cfg/sys

```
[System Menu]
  syslog      - Syslog Menu
  sshd        - SSH Server Menu
  radius      - RADIUS Authentication Menu
  tacacs+     - TACACS+ Authentication Menu
  ntp         - NTP Server Menu
  ssnmp       - System SNMP Menu
  access      - System Access Menu
  date        - Set system date
  time        - Set system time
  timezone    - Set system timezone (daylight savings)
  olddst      - Set system DST for US
  dlight      - Set system daylight savings
  idle        - Set timeout for idle CLI sessions
  notice      - Set login notice
  bannr       - Set login banner
  hprompt     - Enable/disable display hostname (sysName) in CLI prompt
  bootp       - Enable/disable use of BOOTP
  dhcp        - Enable/disable use of DHCP on Mgmt interface
  reminders   - Enable/disable Reminders
  cur         - Display current system-wide parameters
```

This menu provides configuration of switch management parameters such as user and administrator privilege mode passwords, browser-based management settings, and management access list.

The following table describes the System Configuration Menu options.

**Table 79** System Configuration Menu options

Command	Usage
syslog	Displays the Syslog Menu.
sshd	Displays the SSH Server Menu.
radius	Displays the RADIUS Authentication Menu.
tacacs+	Displays the TACACS+ Menu.
ntp	Displays the Network Time Protocol (NTP) Server Menu.
ssnmp	Displays the System SNMP Menu.
access	Displays the System Access Menu.
date	Prompts the user for the system date.
time	Configures the system time using a 24-hour clock format.
timezone	Configures the time zone where the switch resides. You are prompted to select your location (continent, country, region) by the timezone wizard. Once a region is selected, the switch updates the time to reflect local changes to Daylight Savings Time, etc.
olddst	Enables or disables use of the Daylight Saving Time (DST) rules in effect prior to the year 2007. The default value is disabled.

**Table 79** System Configuration Menu options

Command	Usage
<code>dlight enable disable</code>	Enables or disables daylight savings time in the system clock. When enabled, the switch adds an extra hour to the system clock so that it is consistent with the local clock. The default setting is <code>disabled</code> .
<code>idle &lt;1-60&gt;</code>	Sets the idle timeout for CLI sessions, from 1 to 60 minutes. The default value is 5 minutes. This setting affects both the console port and Telnet port.
<code>notice &lt;1-1024 character multi-line&gt; &lt;'-' to end&gt;</code>	Displays login notice immediately before the <code>Enter password: prompt</code> . This notice can contain up to 1024 characters and new lines.
<code>bannr &lt;1-80 characters&gt;</code>	Configures a login banner of up to 80 characters. When a user or administrator logs into the switch, the login banner is displayed. It is also displayed as part of the output from the <code>/info/sys/gen</code> command.
<code>hprompt disable enable</code>	Enables or disables displaying of the host name (system administrator's name) in the command line interface.
<code>bootp disable enable</code>	Enables or disables the use of BOOTP. If you enable BOOTP, the switch will query its BOOTP server for all of the switch IP parameters. The default value is <code>enabled</code> .
<code>dhcp disable enable</code>	Enables or disables Dynamic Host Control Protocol for setting the management IP address on interface 250. When enabled, the IP address obtained from the DHCP server overrides the static IP address. The default value is <code>enabled</code> .
<code>reminders disable enable</code>	Enables or disables reminder messages in the CLI. The default value is <code>enabled</code> .
<code>cur</code>	Displays the current system parameters.

## System host log configuration

**Command:** `/cfg/sys/syslog`

```
[Syslog Menu]
host      - Set IP address of first syslog host
host2     - Set IP address of second syslog host
sever     - Set the severity of first syslog host
sever2    - Set the severity of second syslog host
facil     - Set facility of first syslog host
facil2    - Set facility of second syslog host
console   - Enable/disable console output of syslog messages
log       - Enable/disable syslogging of features
cur       - Display current syslog settings
```



The following table describes the Syslog Configuration Menu options.

**Table 80** Syslog Configuration Menu options

Command	Description
<code>host &lt;IP address&gt;</code>	Sets the IP address of the first syslog host. For example, 100.10.1.1.
<code>host2 &lt;IP address&gt;</code>	Sets the IP address of the second syslog host. For example, 100.10.1.2.
<code>sever &lt;1-7&gt;</code>	Sets the severity level of the first syslog host displayed. The default is 7, which means log all the severity levels.
<code>sever2 &lt;1-7&gt;</code>	Sets the severity level of the second syslog host displayed. The default is 7, which means log all the severity levels.
<code>facil &lt;1-7&gt;</code>	This option sets the facility level of the first syslog host displayed. The range is 0-7. The default is 0.
<code>facil2 &lt;1-7&gt;</code>	This option sets the facility level of the second syslog host displayed. The range is 0-7. The default is 0.
<code>console disable enable</code>	Enables or disables delivering syslog messages to the console. When necessary, disabling console ensures the switch is not affected by syslog messages. It is enabled by default.
<code>log &lt;feature all&gt; &lt;enable disable&gt;</code>	<p>Displays a list of features for which syslog messages can be generated. You can choose to enable/disable specific features or enable/disable syslog on all available features.</p> <p>Features include:</p> <ul style="list-style-type: none"> <li>• console</li> <li>• system</li> <li>• mgmt</li> <li>• cli</li> <li>• stg</li> <li>• vlan</li> <li>• hotlinks</li> <li>• ssh</li> <li>• ntp</li> <li>• ip</li> <li>• web</li> <li>• rmon</li> <li>• ufd</li> <li>• sfd</li> </ul>
<code>cur</code>	Displays the current syslog settings.

# Secure Shell Server configuration

**Command:** /cfg/sys/sshd

```
[SSHD Menu]
interval- Set Interval for generating the RSA server key
scpadm - Set SCP-only admin password
hkeygen - Generate the RSA host key
skeygen - Generate the RSA server key
sshport - Set SSH server port number
ena      - Enable the SCP apply and save
dis      - Disable the SCP apply and save
on       - Turn SSH server ON
off      - Turn SSH server OFF
cur      - Display current SSH server configuration
```

Telnet traffic on the network is not secure. This menu enables Secure Shell (SSH) access from any SSH client. The SSH program securely logs into another computer over a network and executes commands in a secure environment. All data using SSH is encrypted.

**NOTE:** See the *HP 10Gb Ethernet BL-c Switch Application Guide* for information on SSH.

The following table describes the SSHD Configuration Menu options.

**Table 81** SSHD Configuration Menu options

Command	Description
interval <0-24>	Defines interval for auto-generating the RSA server key. The switch will auto-generate the RSA server key at the interval defined in this command. The value of zero (0) means the RSA server key auto-generation is disabled. If the switch has been busy performing any other key generation and the assigned time of interval expires, the RSA server will skip generating the key.
scpadm	Defines the administrator password that is for Secure Copy (SCP) only. The username for this SCP administrator is <i>scpadmin</i> . Typically, SCP is used to copy files securely from one machine to another. In the switch, SCP is used to download and upload the switch configuration using secure channels.
hkeygen	Generates the RSA host keys manually. The switch creates this key automatically while configuring the switch with Secure Shell (SSH). But you can generate the key manually by using this command if you need to overwrite the key for security reasons. The command will take effect immediately without executing the apply command.
skeygen	Generates the RSA server key. The switch creates this key automatically while configuring the switch with Secure Shell (SSH). You can generate the key manually by using this command if you need to overwrite the key for security reasons. The command will take effect immediately without executing the apply command.
sshport <TCP port number>	Sets the SSH server port number.
ena	Enables the SCP apply and save.
dis	Disables the SCP apply and save. This is the default for SCP.
on	Enables the SSH server.

**Table 81** SSHD Configuration Menu options

Command	Description
off	Disables the SSH server. This is the default for the SSH server.
cur	Displays the current SSH server configuration.

## RADIUS server configuration

**Command:** /cfg/sys/radius

```
[RADIUS Server Menu]
prisrv - Set primary RADIUS server address
secsrv - Set secondary RADIUS server address
secret - Set primary RADIUS server secret
secret2 - Set secondary RADIUS server secret
port - Set RADIUS port
retries - Set RADIUS server retries
timeout - Set RADIUS server timeout
bckdoor - Enable/disable RADIUS backdoor for telnet/ssh/http/https
secbd - Enable/disable RADIUS secure backdoor for telnet/ssh/http/https
on - Turn RADIUS authentication ON
off - Turn RADIUS authentication OFF
cur - Display current RADIUS configuration
```

**NOTE:** See the *HP 10Gb Ethernet BL-c Switch Application Guide* for information on RADIUS.

The following table describes the RADIUS Server Configuration Menu options.

**Table 82** RADIUS Server Configuration Menu options

Command	Description
prisrv <IP address>	Sets the primary RADIUS server address.
secsrv <IP address>	Sets the secondary RADIUS server address.
secret <1-32 characters>	This is the shared secret between the switch and the RADIUS server(s).
secret2 <1-32 characters>	This is the secondary shared secret between the switch and the RADIUS server(s).
port <UDP port number>	Enter the number of the User Datagram Protocol (UDP) port to be configured, between 1500-3000. The default is 1645.
retries <1-3>	Sets the number of failed authentication requests before switching to a different RADIUS server. The range is 1-3 requests. The default is 3 requests.
timeout <1-10>	Sets the amount of time, in seconds, before a RADIUS server authentication attempt is considered to have failed. The range is 1-10 seconds. The default is 3 seconds.
bckdoor enable disable	Enables or disables the RADIUS back door for telnet/SSH/HTTP/HTTPS. This command does not apply when secure backdoor (secbd) is enabled.
secbd enable disable	Enables or disables the RADIUS back door using secure password for telnet/SSH/HTTP/HTTPS. This command does not apply when backdoor (telnet) is enabled.

**Table 82** RADIUS Server Configuration Menu options

Command	Description
on	Enables the RADIUS server.
off	Disables the RADIUS server. This is the default.
cur	Displays the current RADIUS server parameters.



**IMPORTANT:** If RADIUS is enabled, you must login using RADIUS authentication when connecting via the console or Telnet/SSH/HTTP/HTTPS. Backdoor for console is always enabled, so you can connect using `noradius` and the administrator password even if the backdoor (`telnet`) or secure backdoor (`secbd`) are disabled.

If Telnet backdoor is enabled (`telnet ena`), type in `noradius` as a backdoor to bypass RADIUS checking, and use the administrator password to log into the switch. The switch allows this even if RADIUS servers are available.

If secure backdoor is enabled (`secbd ena`), type in `noradius` as a backdoor to bypass RADIUS checking, and use the administrator password to log into the switch. The switch allows this only if RADIUS servers are not available.

## TACACS+ server configuration

**Command:** `/cfg/sys/tacacs+`

```
[TACACS+ Server Menu]
prisrv - Set IP address of primary TACACS+ server
secsrv - Set IP address of secondary TACACS+ server
secret - Set secret for primary TACACS+ server
secret2 - Set secret for secondary TACACS+ server
port - Set TACACS+ port number
retries - Set number of TACACS+ server retries
timeout - Set timeout value of TACACS+ server retries
bckdoor - Enable/disable TACACS+ back door for telnet/ssh/http/https
secbd - Enable/disable TACACS+ secure backdoor for telnet/ssh/http/https
cmap - Enable/disable TACACS+ new privilege level mapping
usermap - Set user privilege mappings
on - Enable TACACS+ authentication
off - Disable TACACS+ authentication
cur - Display current TACACS+ settings
```

TACACS+ (Terminal Access Controller Access Control System) is an authentication protocol that allows a remote access server to forward a user's login password to an authentication server to determine whether access can be allowed to a given system. TACACS+ and Remote Authentication Dial-In User Service (RADIUS) protocols are more secure than the TACACS encryption protocol. TACACS+ is described in RFC 1492.

TACACS+ protocol is more reliable than RADIUS, as TACACS+ uses the Transmission Control Protocol (TCP) whereas RADIUS uses the User Datagram Protocol (UDP). Also, RADIUS combines authentication and authorization in a user profile, whereas TACACS+ separates the two operations.

TACACS+ offers the following advantages over RADIUS as the authentication device:

- TACACS+ is TCP-based, so it facilitates connection-oriented traffic.
- It supports full-packet encryption, as opposed to password-only in authentication requests.
- It supports decoupled authentication, authorization, and accounting.

The following table describes the TACACS+ Server Configuration Menu options.

**Table 83** TACACS+ Server Configuration Menu options

Command	Description
<code>prisrv &lt;IP address&gt;</code>	Defines the primary TACACS+ server address.
<code>secsrv &lt;IP address&gt;</code>	Defines the secondary TACACS+ server address.
<code>secret &lt;1-32 characters&gt;</code>	This is the shared secret between the switch and the TACACS+ server(s).
<code>secret2 &lt;1-32 characters&gt;</code>	This is the secondary shared secret between the switch and the TACACS+ server(s).
<code>port &lt;TCP port number&gt;</code>	Enter the number of the TCP port to be configured, between 1 and 65000. The default is 49.
<code>retries &lt;1-3&gt;</code>	Sets the number of failed authentication requests before switching to a different TACACS+ server. The range is 1-3 requests. The default is 3 requests.
<code>timeout &lt;4-15&gt;</code>	Sets the amount of time, in seconds, before a TACACS+ server authentication attempt is considered to have failed. The range is 4-15 seconds. The default is 5 seconds.
<code>bckdoor enable disable</code>	Enables or disables the TACACS+ back door for Telnet, SSH/SCP, or HTTP/HTTPS. Enabling this feature allows you to bypass the TACACS+ servers. It is recommended that you use Secure Backdoor to ensure the switch is secured, because Secure Backdoor disallows access through the back door when the TACACS+ servers are responding. The default value is <code>disabled</code> .
<code>secbd enable disable</code>	Enables or disables TACACS+ secure back door access through Telnet, SSH/SCP, or HTTP/HTTPS only when the TACACS+ servers are not responding. This feature is recommended to permit access to the switch when the TACACS+ servers become unresponsive. If no back door is enabled, the only way to gain access when TACACS+ servers are unresponsive is to use the back door via the console port. The default value is <code>disabled</code> .
<code>cmap enable disable</code>	Enables or disables TACACS+ privilege-level mapping. The default value is <code>disabled</code> .
<code>usermap &lt;0-15&gt; user oper admin none</code>	Maps a TACACS+ authorization level to a switch user level. Enter a TACACS+ authorization level (0-15), followed by the corresponding HP 10GbE switch user level.
<code>on</code>	Enables the TACACS+ server.
<code>off</code>	Disables the TACACS+ server.
<code>cur</code>	Displays current TACACS+ configuration parameters.



**IMPORTANT:** If TACACS+ is enabled, you must login using TACACS+ authentication when connecting via the console or Telnet/SSH/HTTP/HTTPS. Backdoor for console is always enabled, so you can connect using `notacacs` and the administrator password even if the backdoor (`bckdoor`) or secure backdoor (`secbd`) are disabled.

If Telnet backdoor is enabled (`bckdoor ena`), type `notacacs` as a backdoor to bypass TACACS+ checking, and use the administrator password to log into the switch. The switch allows this even if TACACS+ servers are available.

If secure backdoor is enabled (`secbd ena`), type in `notacacs` as a backdoor to bypass TACACS+ checking, and use the administrator password to log into the switch. The switch allows this only if TACACS+ servers are not available.

## NTP server configuration

**Command:** `/cfg/sys/ntp`

```
[NTP Server Menu]
  prisrv   - Set primary NTP server address
  secsrv   - Set secondary NTP server address
  intrval  - Set NTP server resync interval
  on       - Turn NTP service ON
  off      - Turn NTP service OFF
  cur      - Display current NTP configuration
```

This menu enables you to synchronize the switch clock to a Network Time Protocol (NTP) server. By default, this option is disabled.

The following table describes the NTP Server Configuration Menu options.

**Table 84** NTP Server Configuration Menu options

Command	Description
<code>prisrv &lt;IP address&gt;</code> <code>mgt data</code>	Configures the IP addresses of the primary NTP server to which you want to synchronize the switch clock. By default, the <code>mgt</code> option for the management port is used. To use data ports, specify the <code>data</code> option.
<code>secsrv &lt;IP address&gt;</code> <code>mgt data</code>	Configures the IP addresses of the secondary NTP server to which you want to synchronize the switch clock.
<code>intrval &lt;1-44640&gt;</code>	Specifies the interval, that is, how often, in minutes (1-44640), to resynchronize the switch clock with the NTP server. The default is 1440 seconds.
<code>on</code>	Enables the NTP synchronization service.
<code>off</code>	Disables the NTP synchronization service. This is the default.
<code>cur</code>	Displays the current NTP service settings.

# System SNMP configuration

**Command:** /cfg/sys/ssnmp

```
[SNMP Menu]
snmpv3    - SNMPv3 Menu
name      - Set SNMP "sysName"
locn      - Set SNMP "sysLocation"
cont      - Set SNMP "sysContact"
rcomm     - Set SNMP read community string
wcomm     - Set SNMP write community string
timeout   - Set timeout for the SNMP state machine
auth      - Enable/disable SNMP "sysAuthenTrap"
linkt     - Enable/disable SNMP link up/down trap
ufd       - Enable/disable SNMP Uplink Failure Detection trap
cur       - Display current SNMP configuration
```

The switch software supports SNMP-based network management. In SNMP model of network management, a management station (client/manager) accesses a set of variables known as MIBs (Management Information Base) provided by the managed device (agent). If you are running an SNMP network management station on your network, you can manage the switch using the following standard SNMP MIBs:

- MIB II (RFC 1213)
- Ethernet MIB (RFC 1643)
- Bridge MIB (RFC 1493)

An SNMP agent is a software process on the managed device that listens on UDP port 161 for SNMP messages. Each SNMP message sent to the agent contains a list of management objects to retrieve or to modify.

- SNMP parameters that can be modified include:
- System name
- System location
- System contact
- Use of the SNMP system authentication trap function
- Read community string
- Write community string

The following table describes the System SNMP Configuration Menu options.

**Table 85** System SNMP Configuration Menu options

Command	Description
snmpv3	Displays SNMPv3 menu.
name <1-64 characters>	Configures the name for the system. The name can have a maximum of 64 characters.
locn <1-64 characters>	Configures the name of the system location. The location can have a maximum of 64 characters.
cont <1-64 characters>	Configures the name of the system contact. The contact can have a maximum of 64 characters.
rcomm <1-32 characters>	Configures the SNMP read community string. The read community string controls SNMP "get" access to the switch. It can have a maximum of 32 characters. The default read community string is <code>public</code> .

**Table 85** System SNMP Configuration Menu options

Command	Description
wcomm <1-32 characters>	Configures the SNMP write community string. The write community string controls SNMP “set” and “get” access to the switch. It can have a maximum of 32 characters. The default write community string is <code>private</code> .
timeout <1-30>	Sets the timeout value for the SNMP state machine. The range is 1-30 minutes. The default value is 5 minutes.
auth disable enable	Enables or disables the use of the system authentication trap facility. The default setting is disabled.
linkt <port> [disable enable]	Enables or disables the sending of SNMP link up and link down traps. The default setting is enabled.
ufd	Enables or disables the sending of Uplink Failure Detection traps. The default setting is disabled.
cur	Displays the current SNMP configuration.

## SNMPv3 configuration

**Command:** `/cfg/sys/ssnmp/snmpv3`

```
[SNMPv3 Menu]
  usm      - usmUser Table Menu
  view     - vacmViewTreeFamily Table Menu
  access   - vacmAccess Table Menu
  group    - vacmSecurityToGroup Table Menu
  comm     - community Table Menu
  taddr    - targetAddr Table Menu
  tparam   - targetParams Table Menu
  notify   - notify Table Menu
  vlv2     - Enable/disable V1/V2 access
  cur      - Display current SNMPv3 configuration
```

SNMP version 3 (SNMPv3) is an extensible SNMP Framework that supplements the SNMPv2 Framework by supporting the following:

- a new SNMP message format
- security for messages
- access control
- remote configuration of SNMP parameters

For more details on the SNMPv3 architecture please see RFC2271 to RFC2275.



The following table describes the SNMPv3 Configuration Menu options.

**Table 86** SNMPv3 Configuration Menu options

Command	Description
usm <1-16>	Configures a user security model (USM) entry for an authorized user. You can also configure this entry through SNMP. The range is 1-16.
view <1-128>	Configures different MIB views. The range is 1-128.
access <1-32>	Configures access rights. The View-based Access Control Model defines a set of services that an application can use for checking access rights of the user. You need access control when you have to process retrieval or modification request from an SNMP entity. The range is 1-32.
group <1-16>	Configures an SNMP group. A group maps the user name to the access group names and their access rights needed to access SNMP management objects. A group defines the access rights assigned to all names that belong to a particular group. The range is 1-16.
comm <1-16>	Configures a community table entry. The community table contains objects for mapping community strings and version-independent SNMP message parameters. The range is 1-16.
taddr <1-16>	Configures the destination address and user security levels for outgoing notifications. This is also called the transport endpoint. The range is 1-16.
tparam <1-16>	Configures SNMP parameters, consisting of message processing model, security model, security level, and security name information. There may be multiple transport endpoints associated with a particular set of SNMP parameters, or a particular transport endpoint may be associated with several sets of SNMP parameters.
notify <1-16>	Configures a notification index. A notification application typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions. The range is 1-16.
vlv2 disable enable	Enables or disables the access to SNMP version 1 and version 2. This command is enabled by default.
cur	Displays the current SNMPv3 configuration.

## User Security Model configuration

**Command:** /cfg/sys/ssnmp/snmpv3/usm

```
[SNMPv3 usmUser 1 Menu]
  name      - Set USM user name
  auth      - Set authentication protocol
  authpw    - Set authentication password
  priv      - Set privacy protocol
  privpw    - Set privacy password
  del       - Delete usmUser entry
  cur       - Display current usmUser configuration
```

You can make use of a defined set of user identities using this Security Model. An SNMP engine must have the knowledge of applicable attributes of a user.

This menu helps you create a user security model entry for an authorized user. You need to provide a security name to create the USM entry.

The following table describes the User Security Model Configuration Menu options.

**Table 87** User Security Model Configuration Menu options

Command	Description
name <1-32 characters>	Configures a string up to 32 characters long that represents the name of the user. This is the login name that you need in order to access the switch.
auth md5 sha none	Configures the authentication protocol between HMAC-MD5-96 or HMAC-SHA-96. The default algorithm is none.
authpw	Configures your password for authentication. If you selected an authentication algorithm using the above command, you need to provide a password; otherwise you will get an error message during validation.
priv des none	Configures the type of privacy protocol on the switch. The privacy protocol protects messages from disclosure. The options are des (CBC-DES Symmetric Encryption Protocol) or none. If you specify des as the privacy protocol, then be sure that you have selected one of the authentication protocols (MD5 or HMAC-SHA-96). If you select none as the authentication protocol, you will get an error message.
privpw	Configures the privacy password.
del	Deletes the USM user entries.
cur	Displays the USM user entries.

## SNMPv3 View configuration

**Command:** /cfg/sys/ssnmp/snmpv3/view

```
[SNMPv3 vacmViewTreeFamily 1 Menu]
name      - Set view name
tree      - Set MIB subtree(OID) which defines a family of view subtrees
mask      - Set view mask
type      - Set view type
del       - Delete vacmViewTreeFamily entry
cur       - Display current vacmViewTreeFamily configuration
```

The following table describes the SNMPv3 View Configuration Menu options.

**Table 88** SNMPv3 View Configuration Menu options

Command	Description
name <1-32 characters>	Defines the name for a family of view subtrees up to a maximum of 32 characters.
tree <1-64 characters>	Defines the Object Identifier (OID), a string which, when combined with the corresponding mask, defines a family of view subtrees. An example of an OID is 1.3.6.1.2.1.1.1.0
mask <1-32 characters>	Defines the bit mask, which in combination with the corresponding tree defines a family of view subtrees. The mask can have a maximum of 32 characters.
type included excluded	Selects whether the corresponding instances of vacmViewTreeFamilySubtree and vacmViewTreeFamilyMask define a family of view subtrees, which is included in or excluded from the MIB view.

**Table 88** SNMPv3 View Configuration Menu options

Command	Description
del	Deletes the vacmViewTreeFamily group entry.
cur	Displays the current vacmViewTreeFamily configuration.

## View-based Access Control Model configuration

**Command:** /cfg/sys/ssnmp/snmpv3/access

```
[SNMPv3 vacmAccess 1 Menu]
name      - Set group name
model     - Set security model
level     - Set minimum level of security
rview     - Set read view index
wview     - Set write view index
nview     - Set notify view index
del       - Delete vacmAccess entry
cur       - Display current vacmAccess configuration
```

The view-based Access Control Model defines a set of services that an application can use for checking access rights of the user. Access control is needed when the user has to process SNMP retrieval or modification request from an SNMP entity.

The following table describes the User Access Control Configuration Menu options.

**Table 89** View-based Access Control Configuration Menu options

Command	Description
name <1-32 characters>	Defines the name of the group, up to a maximum of 32 characters.
model usm snmpv1 snmpv2	Selects the security model to be used.
level noAuthNoPriv authNoPriv  authPriv	Defines the minimum level of security required to gain access rights. The level noAuthNoPriv means that the SNMP message will be sent without authentication and without using a privacy protocol. The level authNoPriv means that the SNMP message will be sent with authentication but without using a privacy protocol. The authPriv means that the SNMP message will be sent both with authentication and using a privacy protocol.
rview <1-32 characters>	Defines a 32 character long read view name that allows you read access to a particular MIB view. If the value is empty or if there is no active MIB view having this value then no access is granted.
wview <1-32 characters>	Defines a 32 character long write view name that allows you write access to the MIB view. If the value is empty or if there is no active MIB view having this value then no access is granted.
nview <1-32 characters>	Defines a 32 character long notify view name that allows you notify access to the MIB view.
del	Deletes the View-based Access Control entry.
cur	Displays the View-based Access Control configuration.

## SNMPv3 Group configuration

**Command:** /cfg/sys/ssnmp/snmpv3/group

```
[SNMPv3 vacmSecurityToGroup 1 Menu]
model      - Set security model
uname      - Set USM user name
gname      - Set group name
del        - Delete vacmSecurityToGroup entry
cur        - Display current vacmSecurityToGroup configuration
```

The following table describes the SNMPv3 Group Configuration Menu options.

**Table 90** SNMPv3 Group Configuration Menu options

Command	Description
model usm snmpv1 snmpv2	Defines the security model.
uname <1-32 characters>	Sets the user name as defined in /cfg/sys/ssnmp/snmpv3/usm/name. The user name can have a maximum of 32 characters.
gname <1-32 characters>	Configures the name for the access group as defined in /cfg/sys/ssnmp/snmpv3/access/name. The group name can have a maximum of 32 characters.
del	Deletes the vacmSecurityToGroup entry.
cur	Displays the current vacmSecurityToGroup configuration.

## SNMPv3 Community Table configuration

**Command:** /cfg/sys/ssnmp/snmpv3/comm

```
[SNMPv3 snmpCommunityTable 1 Menu]
index      - Set community index
name       - Set community string
uname      - Set USM user name
tag        - Set community tag
del        - Delete communityTable entry
cur        - Display current communityTable configuration
```

This command is used for configuring the community table entry. The configured entry is stored in the community table list in the SNMP engine. This table is used to configure community strings in the Local Configuration Datastore (LCD) of SNMP engine.

The following table describes the SNMPv3 Community Table Configuration Menu options.

**Table 91** SNMPv3 Community Table Configuration Menu options

Command	Description
index <1-32 characters>	Configures the unique index value of a row in this table. The index can have a maximum of 32 characters.
name <1-32 characters>	Configures the name as defined in /cfg/sys/ssnmp/snmpv3/usm/name. The name can have a maximum of 32 characters.
uname <1-32 characters>	Defines a readable 32 character string that represents the corresponding value of an SNMP community name in a security model.

**Table 91** SNMPv3 Community Table Configuration Menu options

Command	Description
tag <1-255 characters>	Configures a tag of up to 255 characters maximum. This tag specifies a set of transport endpoints to which a command responder application sends an SNMP trap.
del	Deletes the community table entry.
cur	Displays the community table configuration.

## SNMPv3 Target Address Table configuration

**Command:** /cfg/sys/ssnmp/snmpv3/taddr

```
[SNMPv3 snmpTargetAddrTable 1 Menu]
  name      - Set target address name
  addr      - Set target transport address IP
  port      - Set target transport address port
  taglist   - Set tag list
  pname     - Set targetParams name
  del       - Delete targetAddrTable entry
  cur       - Display current targetAddrTable configuration
```

This menu allows you to set passwords and display current user statistics. Passwords can be a maximum of 15 characters. To disable a user, set the password to null by simply pressing the **Enter** key when prompted for the password.

The following table describes the SNMPv3 Target Address Table Configuration Menu options.

**Table 92** SNMPv3 Target Address Table Configuration Menu options

Command	Description
name <1-32 characters>	Configures the locally arbitrary, but unique identifier, target address name associated with this entry.
addr <transport address ip>	Configures a transport address IP that can be used in the generation of SNMP traps.
port <transport address port (1-65535)>	Configures a transport address port that can be used in the generation of SNMP traps.
taglist <1-255 characters>	Configures a list of tags (up to 255 characters maximum) that are used to select target addresses for a particular operation.
pname <1-32 characters>	Defines the name as defined in /cfg/sys/ssnmp/snmpv3/tparam/name.
del	Deletes the Target Address Table entry.
cur	Displays the current Target Address Table configuration.

## SNMPv3 Target Parameters Table configuration

**Command:** /cfg/sys/ssnmp/snmpv3/tparam

```
[SNMPv3 snmpTargetParamsTable 1 Menu]
name      - Set targetParams name
mpmodel   - Set message processing model
model     - Set security model
uname     - Set USM user name
level     - Set minimum level of security
del       - Delete targetParamsTable entry
cur       - Display current targetParamsTable configuration
```

You can configure the target parameters entry and store it in the target parameters table in the SNMP engine. This table contains parameters that are used to generate a message. The parameters include the message processing model (for example: SNMPv3, SNMPv2c, SNMPv1), the security model (for example: USM), the security name, and the security level (noAuthNoPriv, authNoPriv, or authPriv).

The following table describes the SNMPv3 Target Parameters Table Configuration Menu options.

**Table 93** SNMPv3 Target Parameters Table Configuration Menu options

Command	Description
name <1-32 characters>	Configures the locally arbitrary, but unique identifier that is associated with this entry.
mpmodel snmpv1   snmpv2c   snmpv3	Configures the message processing model that is used to generate SNMP messages.
model usm   snmpv1   snmpv2	Selects the security model to be used when generating the SNMP messages.
uname <1-32 characters>	Defines the name that identifies the user in the USM table, on whose behalf the SNMP messages are generated using this entry.
level noAuthNoPriv   authNoPriv   authPriv	Selects the level of security to be used when generating the SNMP messages using this entry. The level noAuthNoPriv means that the SNMP message will be sent without authentication and without using a privacy protocol. The level authNoPriv means that the SNMP message will be sent with authentication but without using a privacy protocol. The authPriv means that the SNMP message will be sent both with authentication and using a privacy protocol.
del	Deletes the targetParamsTable entry.
cur	Displays the current targetParamsTable configuration.

## SNMPv3 Notify Table configuration

**Command:** /cfg/sys/ssnmp/snmpv3/notify

```
[SNMPv3 snmpNotifyTable 1 Menu]
name      - Set notify name
tag       - Set notify tag
del       - Delete notifyTable entry
cur       - Display current notifyTable configuration
```

SNMPv3 uses Notification Originator to send out traps. A notification typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions.

The following table describes the SNMPv3 Notify Table Configuration menu options.

**Table 94** SNMPv3 Notify Table Configuration Menu options

Command	Description
name <1-32 characters>	Defines a locally arbitrary but unique identifier associated with this SNMP notify entry.
tag <1-255 characters>	Defines a tag of 255 characters maximum that contains a tag value which is used to select entries in the Target Address Table. Any entry in the snmpTargetAddrTable, that matches the value of this tag, is selected.
del	Deletes the notify table entry.
cur	Displays the current notify table configuration.

## System Access configuration

**Command:** /cfg/sys/access

```
[System Access Menu]
mgmt      - Management Network Definition Menu
user      - User Access Control Menu (passwords)
http      - Enable/disable HTTP (Web) access
https     - HTTPS Web Access Menu
wport     - Set HTTP (Web) server port number
snmp      - Set SNMP access control
tsbbi     - Enable/disable telnet/ssh configuration from BBI
tnet      - Enable/disable Telnet access
tnport    - Set Telnet server port number
tport     - Set the TFTP Port for the system
cur       - Display current system access configuration
```

The following table describes the System Access Configuration menu options.

**Table 95** System Access Configuration Menu options

Command	Description
mgmt	Displays the Management Configuration Menu.
user	Displays the User Access Control Menu.
http disable enable	Enables or disables HTTP (Web) access to the Browser-based Interface. It is enabled by default.
https	Displays the HTTPS Menu.

**Table 95** System Access Configuration Menu options

Command	Description
wport <TCP port number>	Sets the switch port used for serving switch Web content. The default is HTTP port 80.
snmp disable read-only read-write	Disables or provides read-only/write-read SNMP access.
tsbbi enable disable	Enables or disables BBI configuration control s for Telnet and SSH.
tnet disable enable	Enables or disables Telnet access. You see this command only if you are connected to the switch through a serial connection. The default setting is enabled.
tnport <TCP port number>	Sets an optional telnet server port number for cases where the server listens for telnet sessions on a non-standard port.
tport <TFTP port number>	Sets an optional telnet server port number for cases where the server listens for TFTP sessions on a non-standard port.
cur	Displays the current system access parameters.

## Management Networks configuration

**Command:** /cfg/sys/access/mgmt

```
[Management Networks Menu]
add      - Add mgmt network definition
rem      - Remove mgmt network definition
cur      - Display current mgmt network definitions
clear    - Clear current mgmt network definitions
```

The following table describes the Management Networks Configuration menu options. You can configure up to 10 management networks on the switch.

**Table 96** Management Network Configuration menu options

Command	Description
add <IP address> <IP mask>	Adds a defined network through which switch access is allowed through Telnet, SNMP, RIP, or the browser-based interface. A range of IP addresses is produced when used with a network mask address. Specify an IP address and mask address in dotted-decimal notation.
rem <IP address> <IP mask>	Removes a defined network, which consists of a management network address and a management network mask address.
cur	Displays the current management networks parameters.
clear	Clears the management network definitions.



## User Access Control configuration

**Command:** /cfg/sys/access/user

```
[User Access Control Menu]
uid      - User ID Menu
eject    - Eject user
usrpw    - Set user password (user)
opw      - Set operator password (oper)
admpw    - Set administrator password (admin)
cur      - Display current user status
```

The following table describes the User Access Control menu options.

**Table 97** User Access Control Configuration menu options

Command	Description
uid <1-10>	Displays the User ID Menu for the selected user.
eject <username>	Ejects the selected user from the switch.
usrpw <1-128 characters>	Sets the user (user) password (maximum 128 characters). The user has no direct responsibility for switch management. He or she can view switch status information and statistics, but cannot make any configuration changes.
opw <1-128 characters>	Sets the operator (oper) password (maximum 128 characters). The operator manages all functions of the switch. He or she can view all switch information and statistics and can reset ports or the entire switch.
admpw <1-128 characters>	Sets the administrator (admin) password (maximum 128 characters). The super user administrator has complete access to all menus, information, and configuration commands on the switch, including the ability to change both the user and administrator passwords.
cur	Displays the current user status.

## User ID configuration

**Command:** /cfg/sys/access/user/uid

```
[User ID 1 Menu]
cos      - Set class of service
name     - Set user name
pswd     - Set user password
ena      - Enable user ID
dis      - Disable user ID
del      - Delete user ID
cur      - Display current user configuration
```

The following table describes the User ID Configuration menu options.

**Table 98** User ID Configuration menu options

Command	Description
cos <user oper admin>	Sets the Class-of-Service to define the user's authority level.
name <1-8 characters>	Defines the user name.
pswd <1-128 characters>	Sets the user password of up to 128 characters maximum.

**Table 98** User ID Configuration menu options

Command	Description
ena	Enables the user ID.
dis	Disables the user ID.
del	Deletes the user ID.
cur	Displays the current user ID parameters.

## HTTPS Access configuration

**Command:** /cfg/sys/access/https

```
[https Menu]
access      - Enable/Disable HTTPS Web access
port        - HTTPS WebServer port number
generate    - Generate self-signed HTTPS server certificate
certSave    - save HTTPS certificate
cur         - Display current SSL Web Access configuration
```

The following table describes the HTTPS Access Configuration Menu options.

**Table 99** HTTPS Access Configuration Menu options

Command	Description
access enable disable	Enables or disables BBI access (Web access) using HTTPS. The default value is disabled.
port <TCP port number>	Defines the HTTPS Web server port number.
generate	<p>Allows you to generate a certificate to connect to the SSL to be used during the key exchange. A default certificate is created when HTTPS is enabled for the first time. The user can create a new certificate defining the information that they want to be used in the various fields. For example:</p> <ul style="list-style-type: none"> <li>• Country Name (2 letter code) [ ]: CA</li> <li>• State or Province Name (full name) [ ]: Ontario</li> <li>• Locality Name (for example, city) [ ]: Ottawa</li> <li>• Organization Name (for example, company) [ ]: Hewlett-Packard</li> <li>• Organizational Unit Name (for example, section) [ ]: ProLiant</li> <li>• Common Name (for example, user's name) [ ]: Mr Smith</li> <li>• Email (for example, email address) [ ]: info@hp.com</li> </ul> <p>You must confirm if you want to generate the certificate. It takes approximately 30 seconds to generate the certificate. Then the switch restarts SSL agent.</p>
certSave	Allows the client, or the Web browser, to accept the certificate and save the certificate to Flash to be used when the switch is rebooted.
cur	Displays the current SSL Web Access configuration.

# Port configuration

**Command:** /cfg/port <port number>

```
[Port 1 Menu]
gig      - Gig Phy Menu
aclqos   - Acl/Qos Configuration Menu
stp      - STP Menu - for PVRST only
8021ppri - Set default 802.1p priority
pvid     - Set default port VLAN id
name     - Set port name
rmon     - Enable/Disable RMON for port
tag      - Enable/disable VLAN tagging for port
tagpvid  - Enable/disable tagging on pvid
brate    - Set BroadCast Threshold
mrate    - Set MultiCast Threshold
drate    - Set Dest. Lookup Fail Threshold
ena      - Enable port
dis      - Disable port
cur      - Display current port configuration
```

This menu enables you to configure settings for individual switch ports. This command is enabled by default.

**NOTE:** Port 17 is reserved for switch management.

The following table describes the Port Configuration Menu options.

**Table 100** Port Configuration Menu options

Command	Description
gig	Displays the Gigabit Ethernet Physical Link Menu.
aclqos	Displays the Access Control List (ACL)/Quality of Service (QoS) configuration menu.
stp	Displays the port PVRST menu.
8021ppri	Configures the port's 802.1p priority level.
pvid <1-4094>	Sets the default VLAN number which will be used to forward frames which are not VLAN tagged. The default number is 1.  VLAN 4095 is reserved for switch management.
name <1-64 characters> none	Sets a name for the port (maximum 64 characters). The assigned port name displays next to the port number on some information and statistics screens.
rmon enable disable	Enables or disables Remote Monitoring for the port. RMON must be enabled for any RMON configurations to function.
tag enable disable	Disables or enables VLAN tagging for this port. It is disabled by default.
tagpvid enable disable	Disables or enables VLAN tag persistence. When disabled, the VLAN tag is removed from packets whose VLAN tag matches the port PVID. The default value is enabled.
brate <0-262143> dis	Limits the number of broadcast packets per second to the specified value. If disabled (dis), the port forwards all broadcast packets.

**Table 100** Port Configuration Menu options

Command	Description
<code>mrate &lt;0-262143&gt; dis</code>	Limits the number of multicast packets per second to the specified value. If disabled ( <code>dis</code> ), the port forwards all multicast packets.
<code>drate &lt;0-262143&gt; dis</code>	Limits the number of unknown unicast packets per second to the specified value. If disabled ( <code>dis</code> ), the port forwards all unknown unicast packets.
<code>ena</code>	Enables the port.
<code>dis</code>	Disables the port. To temporarily disable a port without changing its configuration attributes, see the “Temporarily disabling a port” section later in this chapter.
<code>cur</code>	Displays current port parameters.

## Temporarily disabling a port

To temporarily disable a port without changing its stored configuration attributes, enter the following command at any prompt:

```
Main# /oper/port <port number>/dis
```

Because this configuration sets a temporary state for the port, you do not need to use `apply` or `save`. The port state will revert to its original configuration when the switch is reset. See the “Menu information” section in the “Operations Menu” chapter for other operations-level commands.

## Port link configuration

**Command:** `/cfg/port <port number>/gig`

```
[Gigabit Link Menu]
  speed  - Set link speed
  mode   - Set full or half duplex mode
  fctl   - Set flow control
  auto   - Set auto negotiation
  cur    - Display current gig link configuration
```

Use these menu options to set port parameters for the port link.

Link menu options are described in the following table and display on the Gigabit port configuration menus for the switch. Using these configuration menus, you can set port parameters such as speed, duplex, flow control, and negotiation mode for the port link.

The following table describes the Gigabit Link Configuration Menu options.

**Table 101** Gigabit Link Configuration Menu options

Command	Description
<code>speed 100 10000</code>	Sets the link speed.  All downlink and uplink ports are fixed at 10000 Mbps, and cannot be changed. Management port 17 is fixed at 100 Mbps.
<code>mode</code>	Sets the operating mode, as follows: <ul style="list-style-type: none"><li>• Full-duplex</li></ul> All ports are fixed at full duplex, and cannot be changed.
<code>fctl rx tx both none</code>	Sets the flow control. The choices include: <ul style="list-style-type: none"><li>• Receive (rx) flow control</li><li>• Transmit (tx) flow control</li><li>• Both receive and transmit flow control (default)</li><li>• No flow control</li></ul> Management port 17 is fixed at both, and cannot be changed.
<code>auto on off</code>	Enables or disables auto-negotiation for the port.  All downlink and uplink ports are fixed at 10000 Mbps, and cannot be set to auto-negotiate.
<code>cur</code>	Displays current port parameters.

## Port ACL/QoS configuration

**Command:** `/cfg/port <port number>/aclqos`

```
[Port 20 ACL Menu]
add      - Add ACL or ACL group to this port
rem      - Remove ACL or ACL group from this port
cur      - Display current ACLs for this port
```

The following table describes the port ACL/QoS Configuration Menu options.

**Table 102** Port ACL/QoS Configuration Menu options

Command	Description
<code>add acl &lt;1-384&gt;  grp &lt;1-384&gt;</code>	Assigns an ACL or ACL Group to the port.
<code>rem acl &lt;1-384&gt;  grp &lt;1-384&gt;</code>	Removes an ACL or ACL Group from the port.
<code>cur</code>	Displays current port ACL/QoS parameters.

## Port PVRST configuration

**Command:** `/cfg/port <port number>/stp`

```
[Port 1 STP Menu]
  edge      - Enable/disable edge port (for PVRST only)
  link      - Set port link type (auto, p2p, or shared; default: auto)
              (for PVRST only)
  cur       - Display current port stp configuration
```

The following table describes the port PVRST Configuration Menu options.

**Table 103** Port PVRST Configuration Menu options

Command	Description
edge enable disable	Enables or disables this port as an edge port. An edge port is not connected to a bridge, and can begin forwarding traffic as soon as the link is up. Configure server ports as edge ports (enabled). The default value is enabled.
link auto p2p shared	Defines the type of link connected to the port, as follows: <ul style="list-style-type: none"><li>• auto—Configures the port to detect the link type, and automatically match its settings.</li><li>• p2p—Configures the port for Point-To-Point protocol.</li><li>• shared—Configures the port to connect to a shared medium (usually a hub).</li></ul> The default link type is auto.
cur	Displays current port PVRST parameters.

# Layer 2 configuration

**Command:** /cfg/l2

```
[Layer 2 Menu]
 8021x   - 802.1X Menu
 mrst    - Multiple Spanning Tree/Rapid Spanning Tree Menu
 stp     - Spanning Tree Menu
 fdb     - FDB Menu
 trunk   - Trunk Group Menu
 thash   - IP Trunk Hash Menu
 lacp    - Link Aggregation Control Protocol Menu
 hotlink - Hot Links Menu
 vlan    - VLAN Menu
 pvstcomp - Enable/Disable PVST+ compatibility mode
 bpdugrd - Enable/disable BPDU Guard
 upfast  - Enable/disable Uplink Fast
 update  - UplinkFast station update rate
 cur     - Display current layer 2 parameters
```

The following table describes the Layer 2 Configuration Menu options.

**Table 104** L2 Configuration Menu options

Command	Description
8021x	Displays the 802.1X Configuration Menu.
mrst	Displays the Rapid Spanning Tree/Multiple Spanning Tree Protocol Configuration Menu.
stp	Displays the Spanning Tree Configuration Menu.
fdb	Displays the Forwarding Database Configuration Menu.
trunk <1-12>	Displays the Trunk Group Configuration Menu for the selected trunk.
thash	Displays the IP Trunk Hash Menu.
lacp	Displays the Link Aggregation Control Protocol Menu.
hotlink	Displays the Hot Links Configuration Menu.
vlan <1-4094>	Displays the VLAN Configuration Menu.
pvstcomp enable disable	Enables or disables VLAN tagging of spanning tree BPDUs. The default value is <b>enabled</b> .
bpdugrd enable disable	Enables or disables BPDU guard, to avoid spanning-tree loops on ports with Port Fast Forwarding enabled.
upfast enable disable	Enables or disables Fast Uplink Convergence, which provides rapid Spanning Tree convergence to an upstream switch during failover.  When enabled, this feature increases bridge priorities to 65500 for all STGs and path cost by 3000 for all external STP ports.
update <10-200>	Configures the station update rate, in packets per second. The range is 10-200. The default value is 40.
cur	Displays current Layer 2 parameters.

## 802.1X configuration

**Command:** `/cfg/l2/8021x`

```
[802.1X Configuration Menu]
global    - Global 802.1X configuration menu
port      - Port 802.1X configuration menu
ena       - Enable 802.1X access control
dis       - Disable 802.1X access control
cur       - Show 802.1X configuration
```

This feature allows you to configure the HP 10GbE switch as an IEEE 802.1X Authenticator, to provide port-based network access control. The following table describes the 802.1X Configuration Menu options.

**Table 105** 802.1X Configuration Menu options

Command	Description
<code>global</code>	Displays the global 802.1X Configuration Menu.
<code>port &lt;port number&gt;</code>	Displays the 802.1X Port Menu.
<code>ena</code>	Globally enables 802.1X.
<code>dis</code>	Globally disables 802.1X.
<code>cur</code>	Displays current 802.1X parameters.



## 802.1X Global configuration

**Command:** /cfg/l2/8021x/global

```
[802.1X Global Configuration Menu]
mode      - Set access control mode
qtperiod  - Set EAP-Request/Identity quiet time interval
txperiod  - Set EAP-Request/Identity retransmission timeout
suptmout  - Set EAP-Request retransmission timeout
svrtmout  - Set server authentication request timeout
maxreq    - Set max number of EAP-Request retransmissions
raperiod  - Set reauthentication time interval
reauth    - Set reauthentication status to on or off
default   - Restore default 802.1X configuration
cur       - Display current 802.1X configuration
```

The global 802.1X menu allows you to configure parameters that affect all ports in the switch (except management port 17). The following table describes the 802.1X Global Configuration Menu options.

**Table 106** 802.1X Global Configuration Menu options

Command	Description
mode force-unauth auto force-auth	Sets the type of access control for all ports: <ul style="list-style-type: none"><li>• force-unauth - the port is unauthorized unconditionally.</li><li>• auto - the port is unauthorized until it is successfully authorized by the RADIUS server.</li><li>• force-auth - the port is authorized unconditionally, allowing all traffic.</li></ul> The default value is force-auth.
qtperiod <0-65535>	Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/ Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is 60 seconds.
txperiod <1-65535>	Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame. The default value is 30 seconds.
suptmout <1-65535>	Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet from the authentication server. The default value is 30 seconds.
svrtmout <1-65535>	Sets the time, in seconds, the authenticator waits for a response from the Radius server before declaring an authentication timeout. The default value is 30 seconds. The time interval between transmissions of the RADIUS Access-Request packet containing the supplicant's (client's) EAP-Response packet is determined by the current setting of /cfg/sys/radius/timeout (default is 3 seconds).
maxreq <1-10>	Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is 2.
raperiod <1-604800>	Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled. The default value is 3600 seconds.
reauth on off	Sets the re-authentication status to on or off. The default value is off.
default	Resets the global 802.1X parameters to their default values.
cur	Displays current global 802.1X parameters.

## 802.1X Port configuration

**Command:** /cfg/l2/8021x/port <port number>

```
[802.1X Port Configuration Menu]
mode      - Set access control mode
qtperiod  - Set EAP-Request/Identity quiet time interval
txperiod  - Set EAP-Request/Identity retransmission timeout
suptmout  - Set EAP-Request retransmission timeout
svrtmout  - Set server authentication request timeout
maxreq    - Set max number of EAP-Request retransmissions
raperiod  - Set reauthentication time interval
reauth    - Set reauthentication status to on or off
default   - Restore default 802.1X configuration
global    - Apply current global 802.1X configuration to this port
cur       - Display current 802.1X configuration
```

The 802.1X port menu allows you to configure parameters that affect the selected port in the switch. These settings override the global 802.1X parameters.

The following table describes the 802.1X Port Configuration Menu options.

**Table 107** 802.1X Port Configuration Menu options

Command	Description
mode force-unauth auto force-auth	Sets the type of access control for the port: <ul style="list-style-type: none"><li>• force-unauth—the port is unauthorized unconditionally.</li><li>• auto—the port is unauthorized until it is successfully authorized by the RADIUS server.</li><li>• force-auth—the port is authorized unconditionally, allowing all traffic.</li></ul> The default value is force-auth.
qtperiod <0-65535>	Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/ Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is 60 seconds.
txperiod <1-65535>	Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame. The default value is 30 seconds.
suptmout <1-65535>	Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet from the authentication server. The default value is 30 seconds.
svrtmout <1-65535>	Sets the time, in seconds, the authenticator waits for a response from the RADIUS server before declaring an authentication timeout. The default value is 30 seconds. The time interval between transmissions of the RADIUS Access-Request packet containing the supplicant's (client's) EAP-Response packet is determined by the current setting of /cfg/sys/radius/timeout (default is 3 seconds).
maxreq <1-10>	Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is 2.
raperiod <1-604800>	Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled. The default value is 3600 seconds.

**Table 107** 802.1X Port Configuration Menu options

Command	Description
reauth on off	Sets the re-authentication status to on or off. The default value is off.
default	Resets the global 802.1X parameters to their default values.
global	Applies the global 802.1X parameters to the port.
cur	Displays current 802.1X parameters.

# Rapid Spanning Tree Protocol/ Multiple Spanning Tree Protocol configuration

**Command:** /cfg/l2/mrst

```
[Multiple Spanning Tree Menu]
  cist      - Common and Internal Spanning Tree menu
  name      - Set MST region name
  rev       - Set revision level of this MST region
  maxhop    - Set Maximum Hop Count for MST (4 - 60)
  mode      - Spanning Tree Mode
  on        - Globally turns RSTP/MSTP ON
  off       - Globally turns RSTP/MSTP OFF
  cur       - Display current MST parameters
```

The switch supports the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP). MSTP allows you to map many VLANs to a small number of spanning tree groups, each with its own topology.

MSTP supports up to 32 Spanning Tree Groups on the switch (STG 32 is reserved for switch management). MRST is turned off by default.

**NOTE:** When Multiple Spanning Tree is turned on, VLAN 1 is moved from Spanning Tree Group 1 to the Common Internal Spanning Tree (CIST). When Multiple Spanning Tree is turned off, VLAN 1 is moved back to Spanning Tree Group 1.

The following table describes the Multiple Spanning Tree Configuration Menu options.

**Table 108** Multiple Spanning Tree Configuration Menu options

Command	Description
cist	Displays the Common Internal Spanning Tree (CIST) Menu.
name <1-32 characters>	Configures a name for the MSTP region. All devices within a MSTP region must have the same region name.
rev <0-65535>	Configures the revision level for the MSTP region. The revision level is used as a numerical identifier for the region. All devices within a MSTP region must have the same revision level number. The default value is 1.
maxhop <4-60>	Configures the maximum number of bridge hops a packet may to traverse before it is dropped. The range is from 4 to 60 hops. The default value is 20.
rstp mstp pvrst	Selects the spanning-tree mode, as follows: <ul style="list-style-type: none"><li>• Multiple Spanning Tree mode (mst )</li><li>• Rapid Spanning Tree mode (rstp)</li><li>• Per-VLAN Rapid Spanning Tree (pvrst)</li></ul> The default mode is RSTP.
on	Globally turn RSTP/MSTP ON.  When RSTP is turned on, the configuration parameters for STP group 1 apply to RSTP.
off	Globally turn RSTP/MSTP OFF.
cur	Displays the current RSTP/MSTP configuration.

---

**NOTE:**

- IEEE 802.1w standard-based RSTP implementation runs on one STG (i.e. same as one spanning tree instance) only. As a result, if 'rstp' mode is selected under the `/cfg/mrst/mode` command, then only a single RSTP instance (default for STG 1) is supported for all VLANs, including the Default VLAN 1.
  - If multiple spanning tree instances are required, then select 'mstp' mode so that multiple VLANs are handled by multiple spanning tree instances, as specified by IEEE 802.1s standard-based MSTP implementation.
  - IEEE 802.1s MSTP supports rapid convergence using IEEE 802.1w RSTP.
  - PVST+ does not support rapid convergence in current versions.
- 

**NOTE:**

The following configurations are unsupported:

- HP PVST+ (default Spanning Tree setting) is NOT interoperable with Cisco Rapid PVST+.
- HP MSTP/RSTP (with mode set to either 'mstp' or 'rstp') is NOT interoperable with Cisco Rapid PVST+.

The following configurations are supported:

- HP PVST+ (default Spanning Tree setting) is interoperable with Cisco PVST+.
  - HP MSTP/RSTP (with mode set to 'mstp') is interoperable with Cisco MST/RSTP.
- 

## Common Internal Spanning Tree configuration

**Command:** `/cfg/l2/mrst/cist`

```
[Common Internal Spanning Tree Menu]
brg      - CIST Bridge parameter menu
port     - CIST Port parameter menu
add      - Add VLAN(s) to CIST
default  - Default Common Internal Spanning Tree and Member parameters
cur      - Display current CIST parameters
```

The Common Internal Spanning Tree (CIST) provides compatibility with different MSTP regions and with devices running different Spanning Tree instances. It is equivalent to Spanning Tree Group 0.

The following table describes the commands used to configure Common Internal Spanning Tree Configuration Menu options.

**Table 109** Common Internal Spanning Tree Configuration Menu options

Command	Description
brg	Displays the CIST Bridge Menu.
port <port number>	Displays the CIST Port Menu.
add <1-4095>	Adds VLANs to the CIST. Enter one VLAN per line, and press <b>Enter</b> to add the VLANs.
default	Resets all CIST parameters to their default values.
cur	Displays the current CIST configuration.

## CIST bridge configuration

**Command:** /cfg/l2/mrst/cist/brg

```
[CIST Bridge Menu]
prior   - Set CIST bridge Priority (0-65535)
mxage   - Set CIST bridge Max Age (6-40 secs)
fwd     - Set CIST bridge Forward Delay (4-30 secs)
cur     - Display current CIST bridge parameters
```

CIST bridge parameters are used only when the switch is in MSTP mode. CIST parameters do not affect operation of STP/PVST.

The following table describes the commands used to configure CIST Bridge Configuration Menu options parameters.

**Table 110** CIST Bridge Configuration Menu options

Command	Description
prior <0-65535>	Configures the CIST bridge priority. The bridge priority parameter controls which bridge on the network is the MSTP root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. The range is 0 to 65535, and the default is 32768. This command does not apply to RSTP. See the "Bridge Spanning Tree configuration" section for more information.
mxage <6-40>	Configures the CIST bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the MSTP network. The range is 6 to 40 seconds, and the default is 20 seconds. This command does not apply to RSTP. See the "Bridge Spanning Tree configuration" section for more information.
fwd <4-30>	Configures the CIST bridge forward delay parameter. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the listening state to the learning state and from the learning state to the forwarding state. The range is 4 to 30 seconds, and the default is 15 seconds. This command does not apply to RSTP. See the "Bridge Spanning Tree configuration" section for more information.
cur	Displays the current CIST bridge configuration.

## CIST port configuration

**Command:** /cfg/l2/mrst/cist/port <port number>

```
[CIST Port 1 Menu]
prior    - Set port Priority (0-240)
cost     - Set port Path Cost (1-200000000)
hello    - Set CIST port Hello Time (1-10 secs)
link     - Set MSTP link type (auto, p2p, or shared; default: auto)
edge     - Enables or disables this port as an edge port
on       - Turn port's Spanning Tree ON
off      - Turn port's Spanning Tree OFF
cur      - Display current port Spanning Tree parameters
```

CIST port parameters are used to modify MRST operation on an individual port basis. CIST parameters do not affect operation of STP/PVST.

For each port, CIST is turned on by default. Port parameters include:

- Port priority
- Port path cost
- Port Hello time
- Link type
- Edge
- On and off
- Current port configuration

The port option of MRST is turned on by default.

The following table describes the commands used to configure CIST Port Configuration Menu options.

**Table 111** CIST Port Configuration Menu options

Command	Description
prior <0-240>	Configures the CIST port priority. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. The range is 0 to 240, in steps of 16 (0, 16, 32...), and the default is 128.
cost <1-200000000>	Configures the CIST port path cost. The port path cost is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. The default for Gigabit ports is 20000, and for 10Gb ports is 2000.
hello <1-10>	Configures the CIST port Hello time. The Hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge Hello value. The range is 1 to 10 seconds, and the default is 2 seconds.
link auto p2p shared	Defines the type of link connected to the port, as follows: <ul style="list-style-type: none"><li>• auto—Configures the port to detect the link type, and automatically match its settings.</li><li>• p2p—Configures the port for Point-To-Point protocol.</li><li>• shared—Configures the port to connect to a shared medium (usually a hub).</li></ul> The default link type is auto.

**Table 111** CIST Port Configuration Menu options

Command	Description
edge disable enable	Enables or disables this port as an edge port. An edge port is not connected to a bridge, and can begin forwarding traffic as soon as the link is up. Configure server ports as edge ports (enabled). This command is disabled by default.
on	Enables CIST on the port.
off	Disables CIST on the port.
cur	Displays the current CIST port configuration.

## Spanning Tree configuration

**Command:** /cfg/l2/stp <1-128>

```
[Spanning Tree Group 1 Menu]
  brg      - Bridge parameter menu
  port     - Port parameter menu
  add      - Add VLAN(s) to Spanning Tree Group
  remove   - Remove VLAN(s) from Spanning Tree Group
  clear    - Remove all VLANs from Spanning Tree Group
  on       - Globally turn Spanning Tree ON
  off      - Globally turn Spanning Tree OFF
  default  - Default Spanning Tree and Member parameters
  cur      - Display current bridge parameters
```

The HP 10GbE switch supports the IEEE 802.1D Spanning Tree Protocol (STP) and Cisco proprietary PVST and PVST+ protocols. You can configure up to 127 spanning tree groups on the switch (STG 128 is reserved for switch management). Spanning Tree is turned on by default.

**NOTE:** When RSTP is turned on, only STP group 1 can be configured.

The following table describes the Spanning Tree Configuration Menu options.

**Table 112** Spanning Tree Configuration Menu options

Command	Description
brg	Displays the Bridge Spanning Tree Menu.
port <port number>	Displays the Spanning Tree Port Menu.
add <1-4094>	Associates a VLAN with a spanning tree and requires an external VLAN ID as a parameter.
remove <1-4094>	Breaks the association between a VLAN and a spanning tree and requires an external VLAN ID as a parameter.
clear	Removes all VLANs from a spanning tree.
on	Globally enables Spanning Tree Protocol.
off	Globally disables Spanning Tree Protocol.
default	Restores a spanning tree instance to its default configuration.



**Table 112** Spanning Tree Configuration Menu options

Command	Description
cur	Displays current Spanning Tree Protocol parameters.

## Bridge Spanning Tree configuration

**Command:** /cfg/l2/stp/brg

```
[Bridge Spanning Tree Menu]
prior   - Set bridge Priority [0-65535]
hello   - Set bridge Hello Time [1-10 secs]
mxage   - Set bridge Max Age (6-40 secs)
fwd     - Set bridge Forward Delay (4-30 secs)
cur     - Display current bridge parameters
```

Spanning tree bridge parameters can be configured for each Spanning Tree Group. STP bridge parameters include:

- Bridge priority
- Bridge hello time
- Bridge maximum age
- Forwarding delay
- Current bridge configuration

The following table describes the Bridge Spanning Tree Configuration Menu options.

**Table 113** Bridge Spanning Tree Configuration Menu options

Command	Description
prior <0-65535>	<p>Configures the bridge priority. The bridge priority parameter controls which bridge on the network is the STP root bridge.</p> <p>To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. The range is 0 to 65535, and the default is 32768.</p> <p>RSTP/MSTP: The range is 0 to 61440, in steps of 4096 (0, 4096, 8192...), and the default is 32768.</p> <p>This command does not apply to MSTP. See the "Common Internal Spanning Tree configuration" section for more information.</p>
hello <1-10>	<p>Configures the bridge hello time. The hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU).</p> <p>Any bridge that is not the root bridge uses the root bridge hello value. The range is 1 to 10 seconds, and the default is 2 seconds.</p> <p>This command does not apply to MSTP. See the "Common Internal Spanning Tree configuration" section for more information.</p>
mxage <6-40>	<p>Configures the bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the STP network. The range is 6 to 40 seconds, and the default is 20 seconds.</p> <p>This command does not apply to MSTP. See the "Common Internal Spanning Tree configuration" section for more information.</p>

**Table 113** Bridge Spanning Tree Configuration Menu options

Command	Description
<code> fwd &lt;4-30&gt;</code>	Configures the bridge forward delay parameter. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the listening state to the learning state and from the learning state to the forwarding state. The range is 4 to 30 seconds, and the default is 15 seconds.  This command does not apply to MSTP. See the “Common Internal Spanning Tree configuration” section for more information.
<code> cur</code>	Displays the current bridge STP parameters.

When configuring STP bridge parameters, the following formulas must be used:

- $2*(fwd-1) \geq mxage$
- $2*(hello+1) \leq mxage$

## Spanning Tree port configuration

**Command:** `/cfg/l2/stp <1-128>/port <port number>`

```
[Spanning Tree Port 1 Menu]
prior   - Set port Priority (0-255)
cost    - Set port Path Cost (1-65535 (802.1d) /
          1-200000000 (MSTP/RSTP)/0 for auto)
link    - Set port link type (auto, p2p, or shared; default: auto)
edge    - Enables or disables this port as an edge port
fastfwd - Enable/disable Port Fast Forwarding mode
on      - Turn port's Spanning Tree ON
off     - Turn port's Spanning Tree OFF
cur     - Display current port Spanning Tree parameters
```

The default configuration for STP/PVST+ is **off** for downlink ports (1-16) and the management port (17), and **on** for uplink ports (18-21). The default configuration for RSTP/MSTP is Spanning Tree **off** for all downlink ports (1-16) and the management port (17), and **on** for all uplink ports (18-21), with downlink ports configured as **edge** ports.

Spanning tree port parameters are used to modify STP operation on an individual port basis. STP port parameters include:

- Port priority
- Port path cost

The following table describes the Spanning Tree Port Configuration Menu options.

**Table 114** Spanning Tree Port Configuration Menu options

Command	Description
<code>prior &lt;0-255&gt;</code>	<p>Configures the port priority. The port priority helps determine which bridge port becomes the designated port.</p> <p>In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.</p> <p>The range is 0 to 255, and the default is 128.</p> <p>RSTP/MSTP: The range is 0 to 240, in steps of 16 (0, 16, 32...) and the default is 128.</p>
<code>cost &lt;1-65535&gt;</code>	<p>Configures the port path cost. The port path cost is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost.</p> <p>The range is 1 to 65535. The default is 100 for 10Mb ports, 10 for 100 Mb ports, 4 for Gigabit ports, and 2 for 10Gb ports.</p> <p>A value of 0 indicates that the default cost will be computed for an auto-negotiated link speed.</p> <p>RSTP/MSTP: The range is 1 – 2000000000, and the default is 20000 for Gigabit ports, 2000 for 10Gb ports.</p>
<code>link auto p2p shared</code>	<p>Defines the type of link connected to the port, as follows:</p> <ul style="list-style-type: none"> <li>• <code>auto</code>—Configures the port to detect the link type, and automatically match its settings.</li> <li>• <code>p2p</code>—Configures the port for Point-To-Point protocol.</li> <li>• <code>shared</code>—Configures the port to connect to a shared medium (usually a hub).</li> </ul> <p>This command only applies when RSTP is turned on. See the “Common Internal Spanning Tree configuration” section for more information.</p>
<code>edge disable enable</code>	<p>Enables or disables this port as an edge port. An edge port is not connected to a bridge, and can begin forwarding traffic as soon as the link is up. Configure server ports as edge ports (enabled).</p> <p>This command only applies when RSTP is turned on. See the “Common Internal Spanning Tree configuration” section for more information.</p>
<code>fastfwd disable enable</code>	Enables or disables Port Fast Forward on the port.
<code>on</code>	Enables STP on the port.
<code>off</code>	Disables STP on the port.
<code>cur</code>	Displays the current STP port parameters.

## Forwarding Database configuration

**Command:** /cfg/l2/fdb

```
[FDB Menu]
static      - Static FDB Menu
aging       - Configure FDB aging value
cur         - Display current FDB configuration
```

The following table describes the Forwarding Database Configuration Menu options.

**Table 115** FDB Configuration Menu options

Command	Description
static	Displays the Static FDB Configuration Menu.
aging <0-65535>	Configures the aging value for FDB entries. The default value is 300.
cur	Displays current FDB parameters.

## Static FDB configuration

**Command:** /cfg/l2/fdb/static

```
[Static FDB Menu]
add          - Add a permanent FDB entry
del          - Delete a static FDB entry
clear        - Clear static FDB entries
cur          - Display current static FDB configuration
```

The following table describes the Static FDB Configuration Menu options.

**Table 116** Static FDB Configuration Menu options

Command	Description
add <MAC address> <VLAN> <port>	Adds a static entry to the forwarding database.
del <MAC address> <VLAN>	Deletes a static entry from the forwarding database.
clear mac <MAC Address> VLAN <1-4095>  Port <port number> All	Clears specified static FDB entries from the forwarding database, as follows: <ul style="list-style-type: none"><li>• MAC address</li><li>• VLAN</li><li>• Port</li><li>• All</li></ul>
cur	Displays current static FDB parameters.

## Trunk configuration

**Command:** /cfg/l2/trunk <1-12>

```
[Trunk group 1 Menu]
add      - Add port to trunk group
rem      - Remove port from trunk group
ena      - Enable trunk group
dis      - Disable trunk group
del      - Delete trunk group
cur      - Display current Trunk Group configuration
```

Trunk groups can provide super-bandwidth connections between switches or other trunk capable devices. A trunk is a group of ports that act together, combining their bandwidth to create a single, larger port.

Up to 12 trunk groups can be configured on the switch, with the following restrictions.

- Any physical switch port can belong to no more than one trunk group.
- Up to six ports can belong to the same trunk group.
- All ports in a trunk must have the same configuration for speed, flow control, and auto negotiation.
- Trunking from other devices must comply with Cisco® EtherChannel® technology.

**NOTE:** See the *HP 10Gb Ethernet BL-c Switch Application Guide* for information on how to use port trunks.

The following table describes the Trunk Group Configuration Menu options.

**Table 117** Trunk Group Configuration Menu options

Command	Description
add <port number>	Adds a physical port to the current trunk group.
rem <port number>	Removes a physical port from the current trunk group.
ena	Enables the current trunk group.
dis	Turns the current trunk group off.
del	Removes the current trunk group configuration.
cur	Displays current trunk group parameters.

## IP Trunk Hash configuration

**Command:** /cfg/l2/thash

```
[IP Trunk Hash Menu]
  set      - IP Trunk Hash Settings Menu
  cur      - Display current IP trunk hash configuration
```

The following table describes the IP Trunk Hash Configuration Menu options.

**Table 118** IP Trunk Hash Configuration Menu options

Command	Description
set	Displays the Trunk Hash Settings menu.
cur	Display current trunk hash configuration.

## Layer 2 IP Trunk Hash configuration

**Command:** /cfg/l2/thash/set

```
[set IP Trunk Hash Settings Menu]
  smac      - Enable/disable smac hash
  dmac      - Enable/disable dmac hash
  sip       - Enable/disable sip hash
  dip       - Enable/disable dip hash
  cur       - Display current trunk hash setting
```

Trunk hash parameters are set globally for the HP 10GbE switch. You can enable one or two parameters, to configure any of the following valid combinations:

- SMAC (source MAC only)
- DMAC (destination MAC only)
- SIP (source IP only)
- DIP (destination IP only)
- SIP + DIP (source IP and destination IP)
- SMAC + DMAC (source MAC and destination MAC)

The following table describes the IP Trunk Hash Configuration Menu options.

**Table 119** IP Trunk Hash Set Menu options

Command	Description
smac enable disable	Enable or disable trunk hashing on the source MAC.
dmac enable disable	Enable or disable trunk hashing on the destination MAC.
sip enable disable	Enable or disable trunk hashing on the source IP.
dip enable disable	Enable or disable trunk hashing on the destination IP.
cur	Display current trunk hash configuration.

# Link Aggregation Control Protocol configuration

**Command:** /cfg/l2/lacp

```
[LACP Menu]
  sysprio - Set LACP system priority
  timeout - Set LACP system timeout scale for timing out partner info
  port    - LACP port Menu
  cur     - Display current LACP configuration
```

The following table describes the LACP Configuration Menu options.

**Table 120** LACP Configuration Menu options

Command	Description
sysprio <1-65535>	Defines the priority value (1 through 65535) for the switch. Lower numbers provide higher priority. The default value is 32768.
timeout short long	Defines the timeout period before invalidating LACP data from a remote partner. Choose short (3 seconds) or long (90 seconds). The default value is long.  HP recommends that you use a timeout value of long, to reduce LACPDU processing. If your switch's CPU utilization rate remains at 100% for periods of 90 seconds or more, consider using static trunks instead of LACP.
port <port number>	Displays the LACP Port menu.
cur	Display current LACP configuration.

## LACP Port configuration

**Command:** /cfg/l2/lacp/port <port number>

```
[LACP Port 2 Menu]
  mode    - Set LACP mode
  prio    - Set LACP port priority
  adminkey - Set LACP port admin key
  cur     - Display current LACP port configuration
```

The following table describes the LACP Port Configuration Menu options.

**Table 121** LACP Port Configuration Menu options

Command	Description
mode off active passive	Set the LACP mode for this port, as follows: <ul style="list-style-type: none"><li>• off—Turn LACP off for this port. You can use this port to manually configure a static trunk. The default value is off.</li><li>• active—Turn LACP on and set this port to active. Active ports initiate LACPDUs.</li><li>• passive—Turn LACP on and set this port to passive. Passive ports do not initiate LACPDUs, but respond to LACPDUs from active ports.</li></ul>
prio <1-65535>	Sets the priority value for the selected port. Lower numbers provide higher priority. The default is 128.

**Table 121** LACP Port Configuration Menu options

Command	Description
adminkey <1-65535>	Set the admin key for this port. Only ports with the same admin key and oper key (operational state generated internally) can form a LACP trunk group.
cur	Displays the current LACP configuration for this port.

## VLAN configuration

**Command:** /cfg/l2/vlan <1-4094>

```
[VLAN 1 Menu]
  name      - Set VLAN name
  stg       - Assign VLAN to a Spanning Tree Group
  add       - Add port to VLAN
  rem       - Remove port from VLAN
  def       - Define VLAN as list of ports
  ena       - Enable VLAN
  dis       - Disable VLAN
  del       - Delete VLAN
  cur       - Display current VLAN configuration
```

The commands in this menu configure VLAN attributes, change the status of the VLAN, delete the VLAN, and change the port membership of the VLAN.

By default, the VLAN menu option is disabled except VLAN 1, which is always enabled. The HP 10GbE switch supports a maximum of 1,000 VLANs. VLAN 4095 is reserved for switch management.

**NOTE:** See the *HP 10Gb Ethernet BL-c Switch Application Guide* for information on VLANs.

The following table describes the VLAN Configuration Menu options.

**Table 122** VLAN Configuration Menu options

Command	Description
name <1-32 characters>	Assigns a name to the VLAN or changes the existing name. The default VLAN name is the first one.
stg <1-127>	Assigns a VLAN to a spanning tree group. If MSTP is used, the range is 0-32 (0 = CIST).
add <port number>	Adds ports to the VLAN membership.
rem <port number>	Removes ports from the VLAN membership.
def <list of port numbers>	Defines which ports are members of this VLAN. Every port must be a member of at least one VLAN. By default, it defines ports to VLAN 1.
ena	Enables this VLAN.
dis	Disables this VLAN without removing it from the configuration.



**Table 122** VLAN Configuration Menu options

Command	Description
del	Deletes this VLAN.
cur	Displays the current VLAN configuration.



**IMPORTANT:** All ports must belong to at least one VLAN. Any port which is removed from a VLAN and which is not a member of any other VLAN is automatically added to default VLAN #1. You cannot remove a port from VLAN #1 if the port has no membership in any other VLAN. Also, you cannot add a port to more than one VLAN unless the port has VLAN tagging turned on. See the tag command, in the “Port configuration” section earlier in this chapter.

## Protocol VLAN configuration

**Command:** /cfg/l2/vlan x/pvlan x

```
[VLAN 1 Protocol 1 Menu]
  pty      - Set protocol type
  protocol - Select a predefined protocol
  prio     - Set priority to protocol
  add      - Add port to PVLAN
  rem      - Remove port from PVLAN
  ports    - Add/Remove a list of ports to/from PVLAN
  tagpvl   - Enable/Disable port tagging for PVLAN
  taglist  - Enable tagging a port list for PVLAN
  ena      - Enable protocol
  dis      - Disable protocol
  del      - Delete protocol
  cur      - Display current PVLAN configuration
```

The following table describes the Protocol VLAN Configuration Menu options.

**Table 123** Protocol VLAN Configuration Menu options

Command	Description
pty <(Ether2 SNAP LLC)> <Ethernet type>	Configures the frame type and the Ethernet type for the selected protocol. Ethernet type consists of a 4-digit (16 bit) hex code, such as 0080 (IPv4).
protocol	Selects a pre-defined protocol, as follows: <ul style="list-style-type: none"> <li>• decEther2</li> <li>• ipv4Ether2</li> <li>• ipv6Ether2</li> <li>• ipx802.2</li> <li>• ipx802.3</li> <li>• ipxEther2</li> <li>• ipxSnap</li> <li>• netbios</li> <li>• rarpEther2</li> <li>• sna802.2</li> <li>• snaEther2</li> <li>• vinesEther2</li> <li>• xnsEther2</li> </ul>

**Table 123** Protocol VLAN Configuration Menu options

Command	Description
prio <0-7>	Configures the priority value for this PVLAN.
add	Adds a port to the selected PVLAN.
rem	Removes a port from the selected PVLAN.
ports	Defines a list of ports that belong to the selected protocol on this VLAN. Enter 0 (zero) to remove all ports.
tagpvl enable disable	Enables or disables port tagging on this PVLAN.
taglist	Defines a list of ports that will be tagged by the selected protocol on this VLAN. Enter <code>empty</code> to disable tagging on all ports by this PVLAN.
ena	Enables the selected protocol on the VLAN.
dis	Disables the selected protocol on the VLAN.
del	Deletes the selected protocol configuration from the VLAN.
cur	Displays the current configuration for this Protocol VLAN.

## Private VLAN configuration

**Command:** /cfg/l2/vlan x/privlan

```
[privlan Menu]
  type      - Set Private-VLAN type
  map       - Associate secondary VLAN with a primary VLAN
  ena       - Enable Private-VLAN
  dis       - Disable Private-VLAN
  cur       - Display current Private-VLAN configuration
```

The following table describes the Private VLAN Configuration Menu options.

**Table 124** Private VLAN Configuration Menu options

Command	Description
type primary isolated community	Defines the VLAN type, as follows: <ul style="list-style-type: none"> <li>• <b>Primary:</b> A Private VLAN must have only one primary VLAN. The primary VLAN carries unidirectional traffic to ports on the isolated VLAN or to community VLAN.</li> <li>• <b>Isolated:</b> The isolated VLAN carries unidirectional traffic from host ports. A Private VLAN may have only one isolated VLAN.</li> <li>• <b>Community:</b> Community VLANs carry upstream traffic from host ports. A Private VLAN may have multiple community VLANs.</li> </ul>
map <2-4094>	Configures Private VLAN mapping between a secondary VLAN (isolated or community) and a primary VLAN. Enter the primary VLAN ID.
ena	Enables the Private VLAN.

**Table 124** Private VLAN Configuration Menu options

Command	Description
dis	Disables the Private VLAN.
cur	Displays current parameters for the Private VLAN.

## Hot Links configuration

**Command:** /cfg/l2/hotlink

```
[Hot Links Menu]
trigger - Trigger Menu
bpdu    - Enable/disable BPDU flood
sndfdb  - Enable/disable FDB update
on       - Globally turn Hot Links ON
off      - Globally turn Hot Links OFF
cur      - Display current Hot Links configuration
```

The following table describes the Hot Links Configuration menu options.

**Table 125** Hot Links Configuration menu options

Command	Description
trigger <1-4>	Displays the Hot Links Trigger menu.
bpdu enable disable	Enables or disables the ability to flood BPDUs on the active Hot Links interface the interface belongs to a Spanning Tree group that is globally turned off. The default value is disabled.
sndfdb enable disable	Enables or disables FDB Update, which allows the GbE2c to send FDB and MAC update packets over the active interface. The default value is disabled.
on	Globally turns Hot Links on. The default value is off.
off	Globally turns Hot Links off.
cur	Displays the current Hot Links configuration.

## Hot Links Trigger configuration

**Command:** /cfg/l2/hotlink/trigger <1-4>

```
[Trigger 1 Menu]
  master    - Master Menu
  backup    - Backup Menu
  fdelay    - Set Forward Delay (secs)
  name      - Set Trigger Name
  preempt   - Enable/disable Preemption
  ena       - Enable Trigger
  dis       - Disable Trigger
  del       - Delete Trigger
  cur       - Display current Trigger configuration
```

The following table describes the Hot Links Trigger Menu options.

**Table 126** Hot Links Trigger menu options

Command	Description
master	Displays the Master interface menu for the selected trigger.
backup	Displays the Backup interface menu for the selected trigger.
fdelay <0-3600>	Configures the Forward Delay interval, in seconds. The default value is 1.
name <text string>	Configures a name for the trigger.
preempt enable disable	Enables or disables pre-emption, which allows the Master interface to transition to the Active state whenever it becomes available. The default option is <b>enabled</b> .
ena	Enables the Hot Links trigger.
dis	Disables the Hot Links trigger.
del	Deletes the Hot Links trigger.
cur	Displays the current Hot Links trigger configuration.

## Hot Links Master configuration

**Command:** /cfg/l2/hotlink/trigger <1-4>/master

```
[Master Menu]
  port      - Set port in Master
  trunk     - Set trunk in Master
  cur       - Display current Master configuration
```

The following table describes the Hot Links Master menu options.

**Table 127** Hot Links Master Menu options

Command	Description
port <port number (0, 18-21)>	Adds the selected port to the Master interface. Enter zero (0) to clear the port.
trunk <trunk group number (1-12)>	Adds the selected trunk group to the Master interface.

**Table 127** Hot Links Master Menu options

Command	Description
cur	Displays the current Master interface configuration.

## Hot Links Backup configuration

**Command:** /cfg/l2/hotlink/trigger <1-4>/backup

```
[Backup Menu]
  port      - Set port in Backup
  trunk     - Set trunk in Backup
  cur       - Display current Backup configuration
```

The following table describes the Hot Links Backup Menu options.

**Table 128** Hot Links Backup menu options

Command	Description
port <port number (0, 18-21)>	Adds the selected port to the Backup interface. Enter zero (0) to clear the port.
trunk <trunk group number (1-12)>	Adds the selected trunk group to the Backup interface.
cur	Displays the current Backup interface configuration.

# Layer 3 configuration

**Command:** /cfg/l3

```
[Layer 3 Menu]
  if      - Interface Menu
  gw      - Default Gateway Menu
  route   - Static Route Menu
  arp     - ARP Menu
  frwd    - Forwarding Menu
  nwf     - Network Filters Menu
  rmap    - Route Map Menu
  rip     - Routing Information Protocol Menu
  ospf    - Open Shortest Path First (OSPF) Menu
  igmp    - IGMP Menu
  dns     - Domain Name System Menu
  bootp   - Bootstrap Protocol Relay Menu
  sm      - ServerMobility Menu
  vrrp    - Virtual Router Redundancy Protocol Menu
  rtrid   - Set router ID
  cur     - Display current IP configuration
```

The following table describes the Layer 3 Configuration Menu options.

**Table 129** L3 Configuration Menu options

Command	Description
if <1-250>	Displays the IP Interface Menu.
gw <1-4, 254>	Displays the IP Default Gateway Menu.
route	Displays the IP Static Route Menu.
arp	Displays the ARP (Address Resolution Protocol) Menu.
frwd	Displays the IP Forwarding Menu.
nwf <1-256>	Displays the Network Filter Configuration Menu.
rmap <1-32>	Displays the Route Map Menu.
rip	Displays the Routing Interface Protocol Menu.
ospf	Displays the OSPF Menu.
igmp	Displays the IGMP Menu.
dns	Displays the IP Domain Name System Menu.
bootp	Displays the Bootstrap Protocol Menu.
sm	Displays the Server Mobility Menu.
vrrp	Displays the Virtual Router Redundancy Configuration Menu.
rtrid <IP address (such as, 192.4.17.101)>	Sets the router ID.
cur	Displays the current IP configuration.

## IP interface configuration

**Command:** /cfg/l3/if <1-250>

```
[IP Interface 1 Menu]
addr      - Set IP address
mask      - Set subnet mask
vlan      - Set VLAN number
relay     - Enable/disable BOOTP relay
ena       - Enable IP interface
dis       - Disable IP interface
del       - Delete IP interface
cur       - Display current interface configuration
```

The switch can be configured with up to 250 IP interfaces. Each IP interface represents the switch on an IP subnet on your network. The IP Interface option is disabled by default.

The following table describes the IP Interface Configuration Menu options.

**Table 130** IP Interface Configuration Menu options

Command	Description
addr <IP address>	Configures the IP address of the switch interface, using dotted decimal notation. For example, 192.2.14.101
mask <IP subnet mask>	Configures the IP subnet address mask for the interface using dotted decimal notation. For example, 255.255.255.0
vlan <1-4094>	Configures the VLAN number for this interface. Each interface can belong to one VLAN, though any VLAN can have multiple IP interfaces in it.
relay disable enable	Enables or disables the BOOTP relay on this interface. The default value is enabled.
ena	Enables this IP interface.
dis	Disables this IP interface.
del	Removes this IP interface.
cur	Displays the current interface settings.

**NOTE:** If you enter an IP address for interface 1, you are prompted to change the BOOTP setting.

## Default Gateway configuration

**Command:** `/cfg/l3/gw <1-4, 254>`

```
[Default gateway 1 Menu]
addr      - Set IP address
intr      - Set interval between ping attempts
retry     - Set number of failed attempts to declare gateway DOWN
arp       - Enable/disable ARP only health checks
ena       - Enable default gateway
dis       - Disable default gateway
del       - Delete default gateway
cur       - Display current default gateway configuration
```

The switch supports up to four gateways, plus the management gateway 254. By default, no gateways are configured on the switch. Enter 1, 2, 3, or 4, or 254 in the command as the *<gateway number>*, depending upon which gateway you want to configure.

The following table describes the Default IP Gateway Configuration Menu options.

**Table 131** Default IP Gateway Configuration Menu options

Command	Description
<code>addr &lt;IP address&gt;</code>	Configures the IP address of the default IP gateway using dotted decimal notation. For example, 192.4.17.44.
<code>intr &lt;0-60&gt;</code>	The switch pings the default gateway to verify that it is up. The <code>intr</code> option sets the time between health checks. The range is from 0 to 60 seconds. The default is 2 seconds.
<code>retry &lt;1-120&gt;</code>	Sets the number of failed health check attempts required before declaring this default gateway inoperative. The range is from 1 to 120 attempts. The default is 8 attempts.
<code>arp disable enable</code>	Enables or disables Address Resolution Protocol (ARP) health checks. This command is disabled by default.
<code>ena</code>	Enables the gateway for use.
<code>dis</code>	Disables the gateway.
<code>del</code>	Deletes the gateway from the configuration.
<code>cur</code>	Displays the current gateway settings.



## IP Static Route configuration

**Command:** /cfg/l3/route

```
[IP Static Route Menu]
add      - Add static route
rem      - Remove static route
cur      - Display current static route configuration
```

The following table describes the Static Route Configuration Menu options.

**Table 132** Static Route Configuration Menu options

Command	Description
add <IP address> <IP subnet mask> <gateway> <interface>	Adds a static route. You will be prompted to enter a destination IP address, destination subnet mask, and gateway address. Enter all addresses using dotted decimal notation.
rem <IP address> <IP subnet mask>	Removes a static route. The destination address of the route to remove must be specified using dotted decimal notation.
cur	Displays the current IP configuration.

## Address Resolution Protocol configuration

**Command:** /cfg/l3/arp

```
[ARP Menu]
static   - Static ARP Menu
rearp    - Set re-ARP period in minutes
cur      - Display current ARP configuration
```

Address Resolution Protocol (ARP) is the TCP/IP protocol that resides within the Internet layer. ARP resolves a physical address from an IP address. ARP queries machines on the local network for their physical addresses. ARP also maintains IP to physical address pairs in its cache memory. In any IP communication, the ARP cache is consulted to see if the IP address of the computer or the router is present in the ARP cache. Then the corresponding physical address is used to send a packet.

The following table describes the ARP Configuration Menu options.

**Table 133** ARP Configuration Menu options

Command	Description
static	Displays the Static ARP Configuration menu.
rearp <2-120>	Defines re-ARP period in minutes. You can set this duration between two and 120 minutes.
cur	Displays the current ARP configurations.

## Static ARP configuration

**Command:** /cfg/l3/arp/static

```
[Static ARP Menu]
add      - Add a permanent ARP entry
del      - Delete an ARP entry
clear    - Clear static ARP entries
cur      - Display current static ARP configuration
```

Static ARP entries are permanent in the ARP cache and do not age out like the ARP entries that are learnt dynamically. Static ARP entries enable the switch to reach the hosts without sending an ARP broadcast request to the network. Static ARPs are also useful to communicate with devices that do not respond to ARP requests. Static ARPs can also be configured on some gateways as a protection against malicious ARP Cache corruption and possible DOS attacks.

The following table describes the Static ARP Configuration Menu options.

**Table 134** Static ARP Configuration Menu options

Command	Description
add <IP address> <MAC address> <VLAN number> <port number>	Adds a permanent ARP entry.
del <IP address (such as, 192.4.17.101)>	Deletes a permanent ARP entry.
clear [<interface number> <VLAN number> <port number> all] <ARP entry number>	Clears static ARP entries.
cur	Displays current static ARP configuration.

## IP Forwarding configuration

**Command:** /cfg/l3/frwd

```
[IP Forwarding Menu]
dirbr    - Enable/disable forwarding directed broadcasts
on        - Globally turn IP Forwarding ON
off       - Globally turn IP Forwarding OFF
cur       - Display current IP Forwarding configuration
```

The following table describes the IP Forwarding Configuration Menu options.

**Table 135** IP Forwarding Configuration Menu options

Command	Description
dirbr disable enable	Enables or disables forwarding directed broadcasts. This command is disabled by default.
on	Enables IP forwarding (routing) on the switch.
off	Disables IP forwarding (routing) on the switch. Forwarding is turned off by default.
cur	Displays the current IP forwarding settings.

## Network Filter configuration

**Command:** /cfg/l3/nwf <1-256>

```
[IP Network Filter 1 Menu]
addr      - IP Address
mask      - IP Subnet mask
enable    - Enable Network Filter
disable   - Disable Network Filter
delete    - Delete Network Filter
current   - Display current Network Filter configuration
```

The following table describes the Network Filter Configuration Menu options.

**Table 136** Network Filter Configuration Menu options

Command	Description
addr <IP address>	Sets the starting IP address for this filter. The default address is 0.0.0.0.
mask <IP subnet mask>	Sets the IP subnet mask that is used with /cfg/l3/nwf/addr to define the range of IP addresses that will be accepted by the peer when the filter is enabled. The default value is 0.0.0.0.
enable	Enables the Network Filter configuration.
disable	Disables the Network Filter configuration.
delete	Deletes the Network Filter configuration.
current	Displays the current the Network Filter configuration.

## Route Map configuration

**Command:** /cfg/l3/rmap <1-32>

```
[IP Route Map 1 Menu]
alist     - Access List number
metric    - Set metric of the matched route
type      - Set OSPF metric-type of the matched route
prec      - Set the precedence of this route map
enable    - Enable route map
disable   - Disable route map
delete    - Delete route map
current   - Display current route map configuration
```

Routing maps control and modify routing information. The map number <1-32> represents the routing map you wish to configure.

The following table describes the Route Map Configuration Menu options.

**Table 137** Route Map Configuration Menu options

Command	Description
alist <1-8>	Displays the Access List menu.
metric <0-16777214> none	Sets the metric of the matched route.

**Table 137** Route Map Configuration Menu options

Command	Description
type 1 2 none	Assigns the type of OSPF metric. The default is type 1. <ul style="list-style-type: none"> <li>1—External routes are calculated using both internal and external metrics.</li> <li>2—External routes are calculated using only the external metrics. Type 2 routes have more cost than Type 2.</li> <li>none—Removes the OSPF metric.</li> </ul>
prec <1-255>	Sets the precedence of the route map. The smaller the value, the higher the precedence. Default value is 10.
enable	Enables the route map.
disable	Disables the route map.
delete	Deletes the route map.
cur	Displays the current route configuration.

## IP Access List configuration

**Command:** /cfg/l3/rmap <1-32>/alist <1-8>

```
[IP Access List 1 Menu]
  nwf      - Network Filter number
  metric   - Metric
  action    - Set Network Filter action
  enable   - Enable Access List
  disable  - Disable Access List
  delete   - Delete Access List
  current  - Display current Access List configuration
```

The route map number <1-32> and the access list number <1-8> represent the IP access list you wish to configure. The following table describes the IP Access List Configuration Menu options.

**Table 138** IP Access List Configuration Menu options

Command	Description
nwf <1-256>	Sets the network filter number.
metric <1-16777214> none	Sets the metric value in the AS-External (ASE) LSA.
action permit deny	Permits or denies action for the access list.
enable	Enables the access list.
disable	Disables the access list.
delete	Deletes the access list.
cur	Displays the current Access List configuration.

# Routing Information Protocol configuration

**Command:** /cfg/l3/rip

```
[Routing Information Protocol Menu]
  if      - RIP Interface Menu
  update  - Set update period in seconds
  redist  - RIP Route Redistribute Menu
  on      - Globally turn RIP ON
  off     - Globally turn RIP OFF
  current - Display current RIP configuration
```

The RIP Menu is used for configuring Routing Information Protocol parameters. This option is turned off by default.

The following table describes the RIP Configuration Menu options.

**Table 139** RIP Configuration Menu options

Command	Description
if <1-249>	Displays the RIP Interface menu.
update <1-120>	Configures the time interval for sending for RIP table updates, in seconds. The default value is 30 seconds.
redist	Displays the RIP Route Redistribute menu.
on	Globally turns RIP on.
off	Globally turns RIP off.
cur	Displays the current RIP configuration.

## RIP Interface configuration

**Command:** /cfg/l3/rip/if <1-249>

```
[RIP Interface 1 Menu]
version - Set RIP version
supply - Enable/disable supplying route updates
listen - Enable/disable listening to route updates
poison - Enable/disable poisoned reverse
split - Enable/disable split horizon
trigg - Enable/disable triggered updates
mcast - Enable/disable multicast updates
default - Set default route action
metric - Set metric
auth - Set authentication type
key - Set authentication key
enable - Enable interface
disable - Disable interface
current - Display current RIP interface configuration
```

The RIP Menu is used for configuring Routing Information Protocol parameters. This option is turned off by default.

**NOTE:** Do not configure RIP version 1 parameters if your routing equipment uses RIP version 2.

The following table describes the RIP Interface Configuration Menu options.

**Table 140** RIP Interface Configuration Menu options

Command	Description
version 1 2 both	Configures the RIP version used by this interface. The default value is version 2.
supply disable enable	When enabled, the switch supplies routes to other routers. This command is enabled by default.
listen disable enable	When enabled, the switch learns routes from other routers. This command is enabled by default.
poison disable enable	When enabled, the switch uses split horizon with poisoned reverse. When disabled, the switch uses only split horizon. The default value is disabled.
split disable enable	Enables or disables split horizon. The default value is enabled.
trigg disable enable	Enables or disables Triggered Updates. Triggered Updates are used to speed convergence. When enabled, Triggered Updates force a router to send update messages immediately, even if it is not yet time for the update message. The default value is enabled.
mcast disable enable	Enables or disables multicast updates of the routing table (using address 224.0.0.9). The default value is enabled.
default none listen supply both	When enabled, the switch accepts RIP default routes from other routers, but gives them lower priority than configured default gateways. When disabled, the switch rejects RIP default routes. The default value is disabled.
metric <1-15>	Configures the route metric, which indicates the relative distance to the destination. The default value is 1.
auth none password	Configures the authentication type. The default is none.

**Table 140** RIP Interface Configuration Menu options

Command	Description
key	Configures the authentication key password.
enable	Enables this RIP interface.
disable	Disables this RIP interface.
cur	Displays the current RIP configuration.

## RIP Route Redistribution configuration

**Command:** /cfg/l3/rip/redist fixed|static|ospf|eospf

```
[RIP Redistribute Fixed Menu]
add      - Add rmap into route redistribution list
rem      - Remove rmap from route redistribution list
export   - Export all routes of this protocol
cur      - Display current route-maps added
```

The following table describes the RIP Route Redistribute Menu options.

**Table 141** RIP Redistribute Configuration Menu options

Command	Description
add <1-32> <1-32> all	Adds selected routing maps to the RIP route redistribution list. To add all the 32 route maps, enter <code>all</code> . To add specific route maps, enter routing map numbers one per line, NULL at the end.  This option adds a route map to the route redistribution list. The routes of the redistribution protocol matched by the route maps in the route redistribution list will be redistributed.
remove <1-32> <1-32> all	Removes the route map from the RIP route redistribution list.  Removes routing maps from the list. To remove all 32 route maps, enter <code>all</code> . To remove specific route maps, enter routing map numbers one per line, NULL at end.
export <1-15> none	Exports the routes of this protocol in which the metric and metric type are specified. To remove a previous configuration and stop exporting the routes of the protocol, enter <code>none</code> .
cur	Displays the current RIP route redistribute configuration.

# Open Shortest Path First configuration

**Command:** /cfg/l3/ospf

```
[Open Shortest Path First Menu]
aindex  - OSPF Area (index) Menu
range   - OSPF Summary Range Menu
if       - OSPF Interface Menu
virt     - OSPF Virtual Links Menu
md5key   - OSPF MD5 Key Menu
host     - OSPF Host Entry Menu
redist   - OSPF Route Redistribute Menu
lsdb     - Set the LSDB limit for external LSA
default  - Export default route information
on       - Globally turn OSPF ON
off      - Globally turn OSPF OFF
cur      - Display current OSPF configuration
```

The following table describes the Open Shortest Path First Menu options.

**Table 142** OSPF Configuration Menu options

Command	Description
aindex <0-2>	Displays the area index menu. This area index does not represent the actual OSPF area number.
range <1-16>	Displays summary routes menu for up to 16 IP addresses.
if <1-249>	Displays the OSPF interface configuration menu.
virt <1-3>	Displays the Virtual Links menu used to configure OSPF for a Virtual Link.
md5key <1-255 characters>	Assigns a string to MD5 authentication key.
host <1-128>	Displays the menu for configuring OSPF for the host routes. Up to 128 host routes can be configured. Host routes are used for advertising network device IP addresses to external networks to perform server load balancing within OSPF. It also makes Area Border Route (ABR) load sharing and ABR failover possible.
redist <fixed static rip>	Displays Route Distribution Menu.
lsdb <0-2000>	Sets the link state database limit. Enter 0 (zero) for no limit.
default <1-16777214> none	Sets one default route among multiple choices in an area. Enter none for no default route.
on	Enables OSPF.
off	Disables OSPF.
cur	Displays the current OSPF configuration settings.



## OSPF Area Index configuration

**Command:** /cfg/l3/ospf/aindex <0-2>

```
[OSPF Area (index) 1 Menu]
  areaid    - Set area ID
  type      - Set area type
  metric    - Set stub area metric
  auth      - Set authentication type
  spf       - Set time interval between two SPF calculations
  enable    - Enable area
  disable   - Disable area
  delete    - Delete area
  cur       - Display current OSPF area configuration
```

The following table describes the Area Index Configuration Menu options.

**Table 143** OSPF Area Index Configuration Menu options

Command	Description
areaid <IP address>	Defines the area ID of the OSPF area number.
type transit stub nssa	Defines the type of area. For example, when a virtual link has to be established with the backbone, the area type must be defined as transit. <ul style="list-style-type: none"><li>• transit—allows area summary information to be exchanged between routing devices. Any area that is not a stub area or NSSA is considered to be transit area.</li><li>• stub—an area where external routing information is not distributed. Typically, a stub area is connected to only one other area.</li><li>• nssa—Not-So-Stubby Area (NSSA) is similar to stub area with additional capabilities. For example, routes originating from within the NSSA can be propagated to adjacent transit and backbone areas. External routes from outside the Autonomous System (AS) can be advertised within the NSSA but are not distributed into other areas.</li></ul>
metric <1-65535>	Configures a stub area to send a numeric metric value. All routes received via that stub area carry the configured metric to potentially influencing routing decisions. Metric value assigns the priority for choosing the switch for default route. Metric type determines the method for influencing routing decisions for external routes.
auth none password md5	Defines the authentication method, as follows: <ul style="list-style-type: none"><li>• none—No authentication required.</li><li>• password—Authenticates simple passwords so that only trusted routing devices can participate.</li><li>• md5—This parameter is used when MD5 cryptographic authentication is required.</li></ul>
spf <0-255>	Sets time interval between two successive SPF (shortest path first) calculations of the shortest path tree using the Dijkstra's algorithm.
enable	Enables the OSPF area.
disable	Disables the OSPF area.
delete	Deletes the OSPF area.
cur	Displays the current OSPF configuration.

## OSPF Summary Range configuration

**Command:** /cfg/l3/ospf/range <1-16>

```
[OSPF Summary Range 1 Menu]
  addr      - Set IP address
  mask      - Set IP mask
  aindex    - Set area index
  hide      - Enable/disable hide range
  enable    - Enable range
  disable   - Disable range
  delete    - Delete range
  cur       - Display current OSPF summary range configuration
```

The following table describes the OSPF Summary Range Configuration Menu options.

**Table 144** OSPF Summary Range Configuration Menu options

Command	Description
addr <IP Address>	Configures the base IP address for the range. For example, 100.10.1.1.
mask <IP address mask>	Configures the IP address mask for the range.
aindex <0-2>	Configures the area index used by the switch.
hide disable enable	Hides the OSPF summary range.
enable	Enables the OSPF summary range.
disable	Disables the OSPF summary range.
delete	Deletes the OSPF summary range.
cur	Displays the current OSPF summary range.

## OSPF Interface configuration

**Command:** /cfg/l3/ospf/if <1-249>

```
[OSPF Interface 1 Menu]
  aindex    - Set area index
  prio      - Set interface router priority
  cost      - Set interface cost
  hello     - Set hello interval in seconds
  dead      - Set dead interval in seconds
  trans     - Set transit delay in seconds
  retrans   - Set retransmit interval in seconds
  key       - Set authentication key
  mdkey     - Set MD5 key ID
  enable    - Enable interface
  disable   - Disable interface
  delete    - Delete interface
  cur       - Display current OSPF interface configuration
```

The following table describes the OSPF Interface Configuration Menu options.

**Table 145** OSPF Interface Configuration Menu options

Command	Description
<code>aindex &lt;0-2&gt;</code>	Configures the OSPF area index.
<code>prio &lt;0-255&gt;</code>	Configures the assigned priority value to the OSPF interfaces. (A priority value of 255 is the highest and 1 is the lowest. A priority value of 0 specifies that the interface cannot be used as Designated Router (DR) or Backup Designated Router (BDR).)
<code>cost &lt;1-65535&gt;</code>	Configures cost set for the selected path—preferred or backup. Usually the cost is inversely proportional to the bandwidth of the interface. Low cost indicates high bandwidth.
<code>hello &lt;1-65535&gt;</code>	Configures the interval in seconds between the <code>hello</code> packets for the interfaces.
<code>dead &lt;1-65535&gt;</code>	Configures the health parameters of a <code>hello</code> packet, which is set for an interval of seconds before declaring a silent router to be down.
<code>trans &lt;1-3600&gt;</code>	Configures the transit delay in seconds.
<code>retra &lt;1-3600&gt;</code>	Configures the retransmit interval in seconds.
<code>key &lt;key string&gt; none</code>	Sets the authentication key to clear the password.
<code>mdkey &lt;1-255&gt; none</code>	Assigns an MD5 key to the interface.
<code>enable</code>	Enables the OSPF interface.
<code>disable</code>	Disables the OSPF interface.
<code>delete</code>	Deletes the OSPF interface.
<code>cur</code>	Displays the current settings for OSPF interface.

## OSPF Virtual Link configuration

**Command:** /cfg/l3/ospf/virt <1-3>

```
[OSPF Virtual Link 1 Menu]
  aindex - Set area index
  hello  - Set hello interval in seconds
  dead   - Set dead interval in seconds
  trans  - Set transit delay in seconds
  retra  - Set retransmit interval in seconds
  nbr    - Set router ID of virtual neighbor
  key    - Set authentication key
  mdkey  - Set MD5 key ID
  enable - Enable interface
  disable - Disable interface
  delete - Delete interface
  cur    - Display current OSPF interface configuration
```

The following table describes the OSPF Virtual Link Configuration Menu options.

**Table 146** OSPF Virtual Link Configuration Menu options

Command	Description
aindex <0-2>	Configures the OSPF area index.
hello <1-65535>	Configures the authentication parameters of a hello packet, which is set to be in an interval of seconds.
dead <1-65535>	Configures the health parameters of a hello packet, which is set to be in an interval of seconds. Default is 40 seconds.
trans <1-3600>	Configures the delay in transit in seconds. Default is one second.
retra <1-3600>	Configures the retransmit interval in seconds. Default is five seconds.
nbr <IP address>	Configures the router ID of the virtual neighbor. Default is 0.0.0.0.
key <password>	Configures the password (up to eight characters) for each virtual link. Default is none.
mdkey <1-255> none	Sets MD5 key ID for each virtual link. Default is none.
enable	Enables OSPF virtual link.
disable	Disables OSPF virtual link.
delete	Deletes OSPF virtual link.
cur	Displays the current OSPF virtual link settings.

## OSPF Host Entry configuration

**Command:** /cfg/l3/ospf/host <1-128>

```
[OSPF Host Entry 1 Menu]
addr      - Set host entry IP address
aindex    - Set area index
cost      - Set cost of this host entry
enable    - Enable host entry
disable   - Disable host entry
delete    - Delete host entry
cur       - Display current OSPF host entry configuration
```

The following table describes the OSPF Host Entry Configuration Menu options.

**Table 147** OSPF Host Entry Configuration Menu options

Command	Description
addr <IP address>	Configures the base IP address for the host entry. For example, 100.10.1.1.
aindex <0-2>	Configures the area index of the host.
cost <1-65535>	Configures the cost value of the host.
enable	Enables OSPF host entry.
disable	Disables OSPF host entry.
delete	Deletes OSPF host entry.
cur	Displays the current OSPF host entries.

## OSPF Route Redistribution configuration

**Command:** /cfg/l3/ospf/redist fixed|static|rip

```
[OSPF Redistribute Fixed Menu]
add      - Add rmap into route redistribution list
rem      - Remove rmap from route redistribution list
export   - Export all routes of this protocol
cur      - Display current route-maps added
```

The following table describes the OSPF Route Redistribution Configuration Menu options.

**Table 148** OSPF Route Redistribution Configuration Menu options

Command	Description
add <1-32> <1-32> all	Adds selected routing maps to the rmap list. To add all the 32 route maps, enter all. To add specific route maps, enter routing map numbers one per line, NULL at the end.  This option adds a route map to the route redistribution list. The routes of the redistribution protocol matched by the route maps in the route redistribution list will be redistributed.
rem <1-32> <1-32> ...  all	Removes the route map from the route redistribution list.  Removes routing maps from the rmap list. To remove all 32 route maps, enter all. To remove specific route maps, enter routing map numbers one per line, NULL at the end.

**Table 148** OSPF Route Redistribution Configuration Menu options

Command	Description
export <1-16777215> 1 2 none	Exports the routes of this protocol as external OSPF AS-external LSAs in which the metric and metric type are specified. To remove a previous configuration and stop exporting the routes of the protocol, enter none.
cur	Displays the current route map settings.

## OSPF MD5 Key configuration

**Command:** /cfg/l3/ospf/md5key <key ID>

```
[OSPF MD5 Key 1 Menu]
key      - Set authentication key
delete   - Delete key
cur      - Display current MD5 key configuration
```

The following table describes the OSPF MD5 Key Configuration Menu options.

**Table 149** OSPF MD5 Key Configuration Menu options

Command	Description
key <1-16 characters>	Sets the authentication key for this OSPF packet.
delete	Deletes the authentication key for this OSPF packet.
cur	Displays the current MD5 key configuration.

## IGMP configuration

**Command:** /cfg/l3/igmp

```
[IGMP Menu]
  snoop      - IGMP Snoop Menu
  mrouter    - Static Multicast Router Menu
  igmpflt    - IGMP Filtering Menu
  on         - Globally turn IGMP ON
  off        - Globally turn IGMP OFF
  cur        - Display current IGMP configuration
```

IGMP Snooping allows the switch to forward multicast traffic only to those ports that request it. IGMP Snooping prevents multicast traffic from being flooded to all ports. The switch learns which server hosts are interested in receiving multicast traffic, and forwards it only to ports connected to those servers.

The following table describes the IGMP Menu options.

**Table 150** IGMP Snoop Menu options

Command	Description
snoop	Displays the IGMP Snoop Menu.
mrouter	Displays the Static Multicast Router Menu.
igmpflt	Displays the IGMP Filtering Menu.
on	Globally turns IGMP on.
off	Globally turns IGMP off.
cur	Displays the current IGMP configuration parameters.

## IGMP snooping configuration

**Command:** /cfg/l3/igmp/snoop

```
[IGMP Snoop Menu]
  igmpv3     - IGMP Version3 Snoop Menu
  timeout    - Set report timeout
  mrto       - Set multicast router timeout
  qintrval   - Set IGMP query interval
  robust     - Set expected packet loss on subnet
  flood      - Flood unregistered IPMC
  aggr       - Aggregate IGMP report
  srcip      - Set source ip to use when proxying GSQ
  add        - Add VLAN(s) to IGMP Snooping
  rem        - Remove VLAN(s) from IGMP Snooping
  clear      - Remove all VLAN(s) from IGMP Snooping
  fastlv     - Enable/disable Fastleave processing in VLAN
  cur        - Display current IGMP Snooping configuration
```

The following table describes the IGMP Snoop Configuration Menu options.

**Table 151** IGMP Snoop Menu options

Command	Description
<code>igmpv3</code>	Displays the IGMPv3 Snooping menu.
<code>timeout &lt;1-255&gt;</code>	Sets the Maximum Response Time (MRT) for IGMP hosts. MRT is one of the parameters used to determine the age out period of the IGMP hosts. Increasing the timeout increases the age out period. The range is from 1 to 255 seconds. The default is 10 seconds.
<code>mrto &lt;1-600&gt;</code>	Configures the age-out period for the IGMP Mrouter in the Mrouter table. If the switch does not receive a General Query from the Mrouter for <code>mrto</code> seconds, the switch removes the multicast router from its Mrouter table. The range is from 1 to 600 seconds. The default is 255 seconds.
<code>qinterval &lt;1-600&gt;</code>	Sets the IGMP router query interval. The range is 1-600 seconds. The default value is 125.
<code>robust &lt;2-10&gt;</code>	Configures the IGMP Robustness variable, which allows you to tune the switch for expected packet loss on the subnet. If the subnet is expected to be lossy (high rate of packet loss), then increase the value. The default value is 2.
<code>flood disable enable</code>	Configures the switch to flood unregistered IP multicast reports to all ports.
<code>aggr disable enable</code>	Enables or disables IGMP Membership Report aggregation.
<code>srcip &lt;IP address&gt;</code>	Configures the source IP address used as a proxy for IGMP Group Specific Queries.
<code>add &lt;1-4094&gt;</code>	Adds the VLAN to IGMP Snooping.
<code>rem &lt;1-4094&gt;</code>	Removes the VLAN from IGMP Snooping.
<code>clear</code>	Removes all VLANs from IGMP Snooping.
<code>fastlv &lt;1-4094&gt; disable enable</code>	Enables or disables FastLeave processing. FastLeave allows the switch to immediately remove a port from the IGMP port list, if the host sends a Leave message, and the proper conditions are met. This command is disabled by default.
<code>ena</code>	Enables IGMP Snooping.
<code>dis</code>	Disables IGMP Snooping.
<code>cur</code>	Displays the current IGMP Snooping parameters.



## IGMPv3 Snooping configuration

**Command:** /cfg/l3/igmp/snoop/igmpv3

```
[IGMP V3 Snoop Menu]
sources - Set the number of sources to snoop in group record
v1v2    - Enable/disable snooping IGMPv1/v2 reports
exclude - Enable/disable snooping EXCLUDE mode reports
ena      - Enable IGMPv3 Snooping
dis      - Disable IGMPv3 Snooping
cur      - Display current IGMP Snooping V3 configuration
```

The following table describes the IGMPv3 Snooping Configuration Menu options.

**Table 152** IGMPv3 Snooping Menu options

Command	Description
sources <1-64>	Configures the maximum number of IGMP multicast sources to snoop from within the group record. Use this command to limit the number of IGMP sources to provide more refined control.
v1v2 enable disable	Enables or disables snooping on IGMP version 1 and version 2 reports. When disabled, the switch drops IGMPv1 and IGMPv2 reports. The default value is enabled.
exclude enable disable	Enables or disables snooping on IGMPv3 Exclude Reports. When disabled, the switch ignores Exclude Reports. The default value is enabled.
ena	Enables IGMP version 3. The default value is <b>disabled</b> .
dis	Disables IGMP version 3.
cur	Displays the current IGMP version 3 parameters.

## IGMP static multicast router configuration

**Command:** /cfg/l3/igmp/mrouter

```
[Static Multicast Router Menu]
add - Add port as Multicast Router Port
rem - Remove port as Multicast Router Port
cur - Display current Multicast Router configuration
```

The following table describes the Static Multicast Router Configuration Menu options.

**NOTE:** When you configure a static multicast router on a VLAN, the process of learning multicast routers is disabled for that VLAN.

**Table 153** IGMP Static Multicast Router Menu

Command	Description
add <port number> <1-4094> <1-3>	Selects a port/VLAN combination on which the static multicast router is connected, and configures the IGMP version (1, 2, or 3) of the multicast router.
remove <port number> <1-4094>	Removes a static multicast router from the selected port/VLAN combination.
cur	Displays the current IGMP Static Multicast Router parameters.

## IGMP filtering configuration

**Command:** /cfg/l3/igmp/igmpflt

```
[IGMP Filter Menu]
filter - IGMP Filter Definition Menu
port - IGMP Filtering Port Menu
ena - Enable IGMP Filtering
dis - Disable IGMP Filtering
cur - Display current IGMP Filtering configuration
```

The following table describes the IGMP Filter Configuration Menu options.

**Table 154** IGMP Filtering Menu options

Command	Description
filter <1-16>	Displays the IGMP Filter Definition Menu.
port <port number>	Displays the IGMP Filtering Port Menu.
ena	Enables IGMP filtering globally.
dis	Disables IGMP Filtering globally.
cur	Displays the current IGMP Filtering parameters.

## IGMP filter definition

**Command:** /cfg/l3/igmp/igmpflt/filter <1-16>

```
[IGMP Filter 1 Definition Menu]
range - Set IP Multicast address range
action - Set filter action
ena - Enable filter
dis - Disable filter
del - Delete filter
cur - Display current IGMP filter configuration
```

The following table describes the IGMP Filter Definition Menu options.

**Table 155** IGMP Filter Definition Menu options

Command	Description
range <IP multicast address> <IP multicast address>	Configures the range of IP multicast addresses for this filter. Enter the first IP multicast address of the ranger, followed by the second IP multicast address of the range.
action allow deny	Allows or denies multicast traffic for the IP multicast addresses specified.
ena	Enables this IGMP filter.
dis	Disables this IGMP filter.
del	Deletes this filter's parameter definitions.
cur	Displays the current IGMP filter.

## IGMP filtering port configuration

**Command:** /cfg/l3/igmp/igmpflt/port <port number>

```
[IGMP Port 20 Menu]
filt - Enable/disable IGMP Filtering on port
add - Add IGMP filter to port
rem - Remove IGMP filter from port
cur - Display current IGMP Filtering Port configuration
```

The following table describes the IGMP Port Filtering Configuration Menu options.

**Table 156** IGMP Filtering Port Menu options

Command	Description
filt enable disable	Enables or disables IGMP Filtering on this port.
add <1-16>	Adds an IGMP filter to this port.
rem <1-16>	Removes an IGMP filter from this port.
cur	Displays the current IGMP filter parameters for this port.

## Domain Name System configuration

**Command:** `/cfg/l3/dns`

```
[Domain Name System Menu]
  prima   - Set IP address of primary DNS server
  secon   - Set IP address of secondary DNS server
  dname   - Set default domain name
  cur     - Display current DNS configuration
```

The Domain Name System (DNS) Configuration Menu is used for defining the primary and secondary DNS servers on your local network, and for setting the default domain name served by the switch services. DNS parameters must be configured prior to using hostname parameters with the `ping`, `tracert`, and `tftp` commands.

The following table describes the Domain Name System (DNS) Configuration Menu options.

**Table 157** Domain Name System (DNS) Configuration Menu options

Command	Description
<code>prima &lt;IP address&gt;</code>	Sets the IP address for your primary DNS server. Use dotted decimal notation. For example, 192.4.17.41.
<code>secon &lt;IP address&gt;</code>	Sets the IP address for your secondary DNS server. If the primary DNS server fails, the configured secondary will be used instead. Enter the IP address using dotted decimal notation. For example, 192.4.17.42.
<code>dname &lt;dotted DNS notation&gt; none</code>	Sets the default domain name used by the switch. For example: <code>mycompany.com</code> .
<code>cur</code>	Displays the current Domain Name System (DNS) settings.

## Bootstrap Protocol Relay configuration

**Command:** `/cfg/l3/bootp`

```
[Bootstrap Protocol Relay Menu]
  addr    - Set IP address of BOOTP server
  addr2   - Set IP address of second BOOTP server
  on      - Globally turn BOOTP relay ON
  off     - Globally turn BOOTP relay OFF
  cur     - Display current BOOTP relay configuration
```

The Bootstrap Protocol (BOOTP) Relay Menu is used to allow hosts to obtain their configurations from a Dynamic Host Configuration Protocol (DHCP) server. The BOOTP configuration enables the switch to forward a client request for an IP address to two DHCP/BOOTP servers with IP addresses that have been configured on the switch.

BOOTP relay is turned off by default.

The following table describes the BOOTP Configuration Menu options.

**Table 158** BOOTP Configuration Menu options

Command	Description
addr <IP address>	Sets the IP address of the BOOTP server. For example, 100.10.1.1.
addr2 <IP address>	Sets the IP address of the secondary BOOTP server. For example, 100.10.1.2.
on	Globally turns on BOOTP relay.
off	Globally turns on BOOTP relay.
cur	Displays the current BOOTP relay configuration.

## Server Mobility configuration

**Command:** /cfg/l3/sm

```
[ServerMobility Menu]
  port      - Server Mobility Port Menu
  default   - Set ServerMobility configuration to factory default
  add       - Add ServerMobility ports
  rem       - Remove ServerMobility ports
  filter    - Enable/Disable DHCP request message filters on ports
  nsmrelay  - Enable/Disable relay on non-ServerMobility ports
  on        - Globally turn ServerMobility ON
  off       - Globally turn ServerMobility OFF
  cur       - Display current ServerMobility configuration
```

The following table describes the Server Mobility Configuration menu options.

**Table 159** Server Mobility Configuration menu options

Command	Description
port <port number>	Displays the Server Mobility port menu.
default	Resets the Server Mobility parameters to their factory default values.
add <port number>	Configures a port as a Server Mobility port.
rem <port number>	Removes the port from Server Mobility.
filter enable disable	Enables or disables filtering DHCP request information on the port. When enabled, DHCP requests from the server are filtered, so that the DHCP server receives only DHCP requests from the HP 1:10 GbE switch.
nsmrelay enable disable	Enables or disables BOOTP Relay for all ports that have Server Mobility disabled. The default value is disabled.
on	Globally turns Server Mobility on.
off	Globally turns Server Mobility off.
cur	Displays the current Server Mobility settings.

## Server Mobility port configuration

**Command:** /cfg/13/sm/port <port number>

```
[Port 20 Menu]
  addback  - Set backup port
  remback  - Remove backup port
  cur      - Display current configuration
```

The following table describes the Server Mobility port Configuration menu options.

**Table 160** Server Mobility Configuration menu options

Command	Description
addback <port number>	Configures a backup port for the selected port. The server connected to the backup port acts as a backup to the server connected to this port. The backup server uses the same IP address as the active server.
remback <port number>	Deletes a backup port for the selected port.
cur	Displays the current Server Mobility port settings.

# Virtual Router Redundancy Protocol configuration

**Command:** /cfg/l3/vrrp

```
[Virtual Router Redundancy Protocol Menu]
vr      - VRRP Virtual Router Menu
group   - VRRP Virtual Router Group Menu
if      - VRRP Interface Menu
track   - VRRP Priority Tracking Menu
on      - Globally turn VRRP ON
off     - Globally turn VRRP OFF
cur     - Display current VRRP configuration
```

Virtual Router Redundancy Protocol (VRRP) support on the HP 10GbE switch provides redundancy between routers in a LAN. This is accomplished by configuring the same virtual router IP address and ID number on each participating VRRP-capable routing device. One of the virtual routers is then elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will assume routing authority and take control of the virtual router IP address.

By default, VRRP is disabled. For more information on VRRP, see the “High Availability” chapter in the *HP 10Gb Ethernet BL-c Switch Application Guide*.

The following table describes the VRRP Configuration Menu options.

**Table 161** VRRP Configuration Menu options

Command	Description
vr <1-250>	Displays the VRRP Virtual Router Menu. This menu is used for configuring virtual routers on this switch.
group	Displays the VRRP virtual router group menu, used to combine all virtual routers together as one logical entity. Group options must be configured when using two or more switches in a hot-standby failover configuration where only one switch is active at any given time.
if <1-249>	Displays the VRRP Virtual Router Interface Menu.
track	Displays the VRRP Tracking Menu. This menu is used for weighting the criteria used when modifying priority levels in the master router election process.
on	Globally enables VRRP on this switch.
off	Globally disables VRRP on this switch.
cur	Displays the current VRRP parameters.

## VRRP Virtual Router configuration

**Command:** /cfg/l3/vrrp/vr <1-250>

```
[VRRP Virtual Router 1 Menu]
track    - Priority Tracking Menu
vrid     - Set virtual router ID
addr     - Set IP address
if       - Set interface number
prio     - Set renter priority
adver    - Set advertisement interval
preem    - Enable/disable preemption
ena      - Enable virtual router
dis      - Disable virtual router
del      - Delete virtual router
cur      - Display current VRRP virtual router configuration
```

This menu is used for configuring virtual routers for this switch. A virtual router is defined by its virtual router ID and an IP address. On each VRRP-capable routing device participating in redundancy for this virtual router, a virtual router will be configured to share the same virtual router ID and IP address.

Virtual routers are disabled by default.

The following table describes the Virtual Router Configuration Menu options.

**Table 162** Virtual Router Configuration Menu options

Command	Description
track	Displays the VRRP Priority Tracking Menu for this virtual router. Tracking is a proprietary extension to VRRP, used for modifying the standard priority system used for electing the master router.
vrid <1-250>	<p>Defines the virtual router ID. This is used in conjunction with <code>addr</code> (below) to define a virtual router on this switch. To create a pool of VRRP-enabled routing devices which can provide redundancy to each other, each participating VRRP device must be configured with the same virtual router: one that shares the same <code>vrid</code> and <code>addr</code> combination.</p> <p>The <code>vrid</code> for standard virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer between 1 and 250. The default value is 1.</p> <p>All <code>vrid</code> values must be unique within the VLAN to which the virtual router's IP interface belongs.</p>
addr <IP address>	Defines the IP address for this virtual router using dotted decimal notation. This is used in conjunction with the <code>vrid</code> (above) to configure the same virtual router on each participating VRRP device. The default address is 0.0.0.0.
if <1-249>	Selects a switch IP interface. If the IP interface has the same IP address as the <code>addr</code> option above, this switch is considered the "owner" of the defined virtual router. An owner has a special priority of 255 (highest) and will always assume the role of master router, even if it must preempt another virtual router which has assumed master routing authority. This preemption occurs even if the <code>preem</code> option below is disabled. The default value is 1.



**Table 162** Virtual Router Configuration Menu options

Command	Description
<code>prio &lt;1-254&gt;</code>	<p>Defines the election priority bias for this virtual server. This can be any integer between 1 and 254. The default value is 100.</p> <p>During the master router election process, the routing device with the highest virtual router priority number wins. If there is a tie, the device with the highest IP interface address wins. If this virtual router's IP address (<code>addr</code>) is the same as the one used by the IP interface, the priority for this virtual router will automatically be set to 255 (highest).</p> <p>When priority tracking is used (<code>/cfg/l3/vrrp/track</code> or <code>/cfg/l3/vrrp/vr #/track</code>), this base priority value can be modified according to a number of performance and operational criteria.</p>
<code>adver &lt;1-255&gt;</code>	<p>Defines the time interval between VRRP master advertisements. This can be any integer between 1 and 255 seconds. The default value is 1.</p>
<code>preem disable enable</code>	<p>Enables or disables master preemption. When enabled, if this virtual router is in backup mode but has a higher priority than the current master, this virtual router will preempt the lower priority master and assume control. Note that even when <code>preem</code> is disabled, this virtual router will always preempt any other master if this switch is the owner (the IP interface address and virtual router <code>addr</code> are the same). By default, this option is enabled.</p>
<code>ena</code>	Enables this virtual router.
<code>dis</code>	Disables this virtual router.
<code>del</code>	Deletes this virtual router from the switch configuration.
<code>cur</code>	Displays the current configuration information for this virtual router.

## VRRP Virtual Router Priority Tracking configuration

**Command:** `/cfg/l3/vrrp/vr <1-250>/track`

```
[VRRP Virtual Router 1 Priority Tracking Menu]
vrs      - Enable/disable tracking master virtual routers
ifs      - Enable/disable tracking other interfaces
ports    - Enable/disable tracking VLAN switch ports
cur      - Display current VRRP virtual router configuration
```

This menu is used for modifying the priority system used when electing the master router from a pool of virtual routers. Various tracking criteria can be used to bias the election results. Each time one of the tracking criteria is met, the priority level for the virtual router is increased by an amount defined through the VRRP Tracking Menu.

Criteria are tracked dynamically, continuously updating virtual router priority levels when enabled. If the virtual router preemption option is enabled, this virtual router can assume master routing authority when its priority level rises above that of the current master.

Some tracking criteria (`vrs`, `ifs`, and `ports` below) apply to standard virtual routers, otherwise called virtual interface routers. A virtual server router is defined as any virtual router whose IP address (`addr`) is the same as any configured virtual server IP address.

The following table describes the Virtual Router Priority Tracking Configuration Menu options.

**Table 163** Virtual Router Priority Tracking Configuration Menu options

Command	Description
<code>vrs disable enable</code>	When enabled, the priority for this virtual router will be increased for each virtual router in master mode on this switch. This is useful for making sure that traffic for any particular client/server pairing are handled by the same switch, increasing routing and load balancing efficiency. This command is disabled by default.
<code>ifs disable enable</code>	When enabled, the priority for this virtual router will be increased for each other IP interface active on this switch. An IP interface is considered active when there is at least one active port on the same VLAN. This helps elect the virtual routers with the most available routes as the master. This command is disabled by default.
<code>ports disable enable</code>	When enabled, the priority for this virtual router will be increased for each active port on the same VLAN. A port is considered active if it has a link and is forwarding traffic. This helps elect the virtual routers with the most available ports as the master. This command is disabled by default.
<code>cur</code>	Displays the current configuration for priority tracking for this virtual router.

## VRRP Virtual Router Group configuration

**Command:** `/cfg/l3/vrrp/group`

```
[VRRP Virtual Router Group Menu]
track      - Priority Tracking Menu
vrid       - Set virtual router ID
if         - Set interface number
prio       - Set renter priority
adver      - Set advertisement interval
preem      - Enable/disable preemption
ena        - Enable virtual router
dis        - Disable virtual router
del        - Delete virtual router
cur        - Display current VRRP virtual router configuration
```

The Virtual Router Group menu is used for associating all virtual routers into a single logical virtual router, which forces all virtual routers on the switch to either be master or backup as a group. A virtual router is defined by its virtual router ID and an IP address. On each VRRP-capable routing device participating in redundancy for this virtual router, a virtual router will be configured to share the same virtual router ID and IP address.

The following table describes the Virtual Router Group Configuration Menu options.

**Table 164** Virtual Router Group Configuration Menu options

Command	Description
<code>track</code>	Displays the VRRP Priority Tracking Menu for the virtual router group. Tracking is a proprietary extension to VRRP, used for modifying the standard priority system used for electing the master router.
<code>vrid &lt;1-250&gt;</code>	Defines the virtual router ID. The <code>vrid</code> for standard virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer between 1 and 250. All <code>vrid</code> values must be unique within the VLAN to which the virtual router's IP interface (see <code>if</code> below) belongs. The default virtual router ID is 1.
<code>if &lt;1-249&gt;</code>	Selects a switch IP interface. The default switch IP interface number is 1.
<code>prio &lt;1-254&gt;</code>	Defines the election priority bias for this virtual router group. This can be any integer between 1 and 254. The default value is 100. During the master router election process, the routing device with the highest virtual router priority number wins. If there is a tie, the device with the highest IP interface address wins. If this virtual router's IP address ( <code>addr</code> ) is the same as the one used by the IP interface, the priority for this virtual router will automatically be set to 255 (highest). When priority tracking is used ( <code>/cfg/l3/vrrp/track</code> or <code>/cfg/l3/vrrp/vr #/track</code> ), this base priority value can be modified according to a number of performance and operational criteria.
<code>adver &lt;1-255&gt;</code>	Defines the time interval between VRRP master advertisements. This can be any integer between 1 and 255 seconds. The default is 1.
<code>preem disable enable</code>	Enables or disables master preemption. When enabled, if the virtual router group is in backup mode but has a higher priority than the current master, this virtual router will preempt the lower priority master and assume control. Note that even when <code>preem</code> is disabled, this virtual router will always preempt any other master if this switch is the owner (the IP interface address and virtual router <code>addr</code> are the same). By default, this option is enabled.
<code>ena</code>	Enables the virtual router group.
<code>dis</code>	Disables the virtual router group.
<code>del</code>	Deletes the virtual router group from the switch configuration.
<code>cur</code>	Displays the current configuration information for the virtual router group.

## VRRP Virtual Router Group Priority Tracking configuration

**Command:** /cfg/l3/vrrp/group/track

```
[Virtual Router Group Priority Tracking Menu]
ifs      - Enable/disable tracking other interfaces
ports    - Enable/disable tracking VLAN switch ports
cur      - Display current VRRP Group Tracking configuration
```

**NOTE:** If Virtual Router Group Tracking is enabled, the tracking option will be available only under group option. The tracking setting for the other individual virtual routers will be ignored.

The following table describes the Virtual Router Group Priority Tracking Configuration Menu options.

**Table 165** Virtual Router Group Priority Tracking Configuration Menu options

Command	Description
ifs disable enable	When enabled, the priority for this virtual router will be increased for each other IP interface active on this switch. An IP interface is considered active when there is at least one active port on the same VLAN. This helps elect the virtual routers with the most available routes as the master. This command is disabled by default.
ports disable enable	When enabled, the priority for this virtual router will be increased for each active port on the same VLAN. A port is considered active if it has a link and is forwarding traffic. This helps elect the virtual routers with the most available ports as the master. This command is disabled by default.
cur	Displays the current configuration for priority tracking for this virtual router.

## VRRP Interface configuration

**Command:** /cfg/l3/vrrp/if <1-249>

```
[VRRP Interface 1 Menu]
auth      - Set authentication types
passw     - Set plain-text password
del       - Delete interface
cur       - Display current VRRP interface configuration
```

This menu is used for configuring VRRP authentication parameters for the IP interfaces used with the virtual routers. The interface-number represents the IP interface on which authentication parameters must be configured.

The following table describes the VRRP Interface Configuration Menu options.

**Table 166** VRRP Interface Configuration Menu options

Command	Description
auth none password	Defines the type of authentication that will be used: none (no authentication), or password (password authentication).
passw <password>	Defines a plain text password up to eight characters long. This password will be added to each VRRP packet transmitted by this interface when password authentication is chosen (see auth above).
del	Clears the authentication configuration parameters for this IP interface. The IP interface itself is not deleted.

**Table 166** VRRP Interface Configuration Menu options

Command	Description
cur	Displays the current configuration for this IP interface's authentication parameters.

## VRRP Tracking configuration

**Command:** /cfg/l3/vrrp/track

[VRRP Tracking Menu]

- vrs - Set priority increment for virtual router tracking
- ifs - Set priority increment for IP interface tracking
- ports - Set priority increment for VLAN switch port tracking
- cur - Display current VRRP Priority Tracking configuration

This menu is used for setting weights for the various criteria used to modify priority levels during the master router election process. Each time one of the tracking criteria is met, the priority level for the virtual router is increased by an amount defined through this menu.

**NOTE:** These priority tracking options only define increment values. These options do not affect the VRRP master router election process until options under the VRRP Virtual Router Priority Tracking Menu are enabled.

The following table describes the VRRP Tracking Configuration Menu options.

**Table 167** VRRP Tracking Configuration Menu options

Command	Description
vrs <0-254>	Defines the priority increment value (0 through 254) for virtual routers in master mode detected on this switch. The default value is 2.
ifs <0-254>	Defines the priority increment value (0 through 254) for active IP interfaces detected on this switch. The default value is 2.
ports <0-254>	Defines the priority increment value (0 through 254) for active ports on the virtual router's VLAN. The default value is 2.
cur	Displays the current configuration of priority tracking increment values.

# Quality of Service configuration

**Command:** /cfg/qos

```
[QoS Menu]
8021p      - 802.1p Menu
```

Use the Quality of Service (QoS) menus to configure the IEEE 802.1p priority value of incoming packets. This allows you to differentiate between various types of traffic, and provide different priority levels. The following table describes the QoS Configuration Menu options.

**Table 168** QoS Configuration Menu options

Command	Description
8021p	Displays 802.1p configuration menu.

## QoS 802.1p configuration

**Command:** /cfg/qos/8021p

```
[802.1p Menu]
priq      - Set priority to COS queue mapping
qweight   - Set weight to a COS queue
numcos    - Set number of COS queue
default   - Reset 802.1p configuration to default values.
cur       - Display current 802.1p configuration
```

This feature provides the HP 10GbE switch the capability to filter IP packets based on the IEEE 802.1p bits in the packet's VLAN header. The 802.1p bits specify the priority that you should give to the packets while forwarding them. The packets with a higher (non-zero) priority bits are given forwarding preference over packets with numerically lower priority bits value.

The following table describes the 802.1p Configuration Menu options.

**Table 169** 802.1p Configuration Menu options

Command	Description
priq <0-7> <queue (0-1)   (0-7)>	Maps the 802.1p priority of to the Class of Service queue (COSq) priority. Enter the 802.1p priority value (0-7); followed by the Class of Service queue that handles the matching traffic.
qweight <queue (0-1)   (0-7)> <weight (0-15)>	Configures the weight of the selected Class of Service queue (COSq). Enter the queue number, followed by the scheduling weight (0-15).
numcos 2   8	Sets the number of Class of Service queues for switch ports. The default value is 2.
default	Resets 802.1p configuration to default values.
cur	Displays the current 802.1p parameters.

# Access Control configuration

**Command:** /cfg/acl

```
[ACL Menu]
acl      - Access Control List Item Config Menu
group    - Access Control List Group Config Menu
cur      - Display current ACL configuration
```

Use this menu to create Access Control Lists (ACLs) and ACL Groups. ACLs define matching criteria used for IP filtering and Quality of Service functions.

The following table describes the Access Control Configuration Menu options.

**Table 170** Access Control Configuration Menu options

Command	Description
acl <1-384>	Displays Access Control List (ACL) configuration menu.
group <1-384>	Displays ACL Group configuration menu.
cur	Displays the current Access Control parameters.

## Access Control List configuration

**Command:** /cfg/acl/acl <1-384>

```
[ACL 1 Menu]
ethernet - Ethernet Header Options Menu
ipv4     - IP Header Options Menu
tcpudp   - TCP/UDP Header Options Menu
meter    - ACL Metering Configuration Menu
re-mark  - ACL Re-mark Configuration Menu
pktfmt   - Set to filter specific packet format types
egrport  - Set to filter for packets egressing this port
action   - Set filter action
stats    - Enable/disable statistics for this acl
reset    - Reset filtering parameters
cur      - Display current filter configuration
```

These menus allow you to define filtering criteria for each Access Control List (ACL). The following table describes the ACL Configuration Menu options.

**Table 171** ACL Configuration Menu options

Command	Description
ethernet	Displays the ACL Ethernet configuration menu.
ipv4	Displays the ACL IP version 4 configuration menu.
tcpudp	Displays the ACL TCP/UDP configuration menu.
meter	Displays the ACL meter configuration menu.
re-mark	Displays the ACL re-mark configuration menu.
pktfmt	Displays the ACL Packet Format configuration menu.

**Table 171** ACL Configuration Menu options

Command	Description
<code>egrport &lt;port number&gt;</code>	Configures the ACL to function on egress packets. The egress port ACL will not match a Layer 2 broadcast or multicast packet. The egress port ACL will not match packets if the destination port is a trunk.
<code>action permit deny setprio &lt;0-7&gt;</code>	Configures a filter action for packets that match the ACL definitions. You can choose to permit (pass) or deny (drop) packets, or set the 802.1p priority for the packets.
<code>stats e d</code>	Enables or disables the statistics collection for the Access Control List.
<code>reset</code>	Resets the ACL parameters to their default values and removes the ACL from all ports to which it is assigned.
<code>cur</code>	Displays the current ACL parameters.

## ACL Ethernet Filter configuration

**Command:** `/cfg/acl/acl <1-384>/ethernet`

```
[Filtering Ethernet Menu]
  smac      - Set to filter on source MAC
  dmac      - Set to filter on destination MAC
  vlan      - Set to filter on VLAN ID
  etype     - Set to filter on ethernet type
  pri       - Set to filter on priority
  reset     - Reset all fields
  cur       - Display current parameters
```

This menu allows you to define Ethernet matching criteria for an ACL. The following table describes the Ethernet Filter Configuration Menu options.

**Table 172** Ethernet Filter Configuration Menu options

Command	Description
<code>smac &lt;MAC address&gt; &lt;MAC mask&gt;</code>	Defines the source MAC address and MAC mask for this ACL. For example: 00:60:cf:40:56:00 ff:ff:ff:ff:ff:fc
<code>dmac &lt;MAC address&gt; &lt;MAC mask&gt;</code>	Defines the destination MAC address and MAC mask for this ACL. For example: 00:60:cf:40:56:00 ff:ff:ff:ff:ff:fc
<code>vlan &lt;1-4095&gt; &lt;VLAN mask (0xfff)&gt;</code>	Defines a VLAN number and mask for this ACL.
<code>etype ARP IP IPv6 MPLS RARP any 0xXXXX</code>	Defines the Ethernet type for this ACL.
<code>pri &lt;0-7&gt;</code>	Defines the Ethernet priority value for the ACL.
<code>reset</code>	Resets Ethernet parameters for the ACL to their default values.
<code>cur</code>	Displays the current Ethernet parameters for the ACL.



## ACL IP Version 4 Filter configuration

**Command:** /cfg/acl/acl <1-384>/ipv4

```
[Filtering IPv4 Menu]
sip      - Set to filter on source IP address
dip      - Set to filter on destination IP address
proto    - Set to filter on protocol
tos      - Set to filter on TOS
reset    - Reset all fields
cur      - Display current parameters
```

This menu allows you to define IPv4 matching criteria for an ACL. The following table describes the IP version 4 Filter Configuration Menu options.

**Table 173** IPv4 Filter Configuration Menu options

Command	Description
<code>sip &lt;IP address&gt; &lt;IP mask&gt;</code>	Defines a source IP address for the ACL. If defined, traffic with this source IP address will match this ACL. Specify an IP address in dotted decimal notation. For example, 100.10.1.1.
<code>dip &lt;IP address&gt; &lt;IP mask&gt;</code>	Defines a destination IP address for the ACL. If defined, traffic with this destination IP address will match this ACL. For example, 100.10.1.2.
<code>proto &lt;0-255&gt;</code>	Defines an IP protocol for the ACL. If defined, traffic from the specified protocol matches this filter. Specify the protocol number. Some of the well-known protocols include: <ul style="list-style-type: none"><li>• 1—icmp</li><li>• 2—igmp</li><li>• 6—tcp</li><li>• 17—udp</li><li>• 89—ospf</li><li>• 112—vrrp</li></ul>
<code>tos &lt;0-255&gt;</code>	Defines a Type of Service value for the ACL. For more information on ToS, see RFC 1340 and 1349.
<code>reset</code>	Resets the IPv4 parameters for the ACL to their default values.
<code>cur</code>	Displays the current IPV4 parameters.

## ACL TCP/UDP Filter configuration

**Command:** /cfg/acl/acl <1-384>/tcpudp

[Filtering TCP/UDP Menu]

- sport - Set to filter on TCP/UDP source port
- dport - Set to filter on TCP/UDP destination port
- flags - Set to filter TCP/UDP flags
- reset - Reset all fields
- cur - Display current parameters

This menu allows you to define TCP/UDP matching criteria for an ACL. The following table describes the TCP/UDP Filter Configuration Menu options.

**Table 174** TCP/UDP Filter Configuration Menu options

Command	Description
sport <1-65535> <port mask>	Defines a source port for the ACL. If defined, traffic with the specified TCP or UDP source port will match this ACL. Specify the port number. Some of the well-known ports include: <ul style="list-style-type: none"><li>• Number—Name</li><li>• 20—ftp-data</li><li>• 21—ftp</li><li>• 22—ssh</li><li>• 23—telnet</li><li>• 25—smtp</li><li>• 37—time</li><li>• 42—name</li><li>• 43—whois</li><li>• 53—domain</li><li>• 69—tftp</li><li>• 70—gopher</li><li>• 79—finger</li><li>• 80—http</li></ul>
dport <1-65535>	Defines a destination port for the ACL. If defined, traffic with the specified TCP or UDP destination port will match this ACL. Specify the port number, just as with <code>sport</code> above.
flags <value (0x0-0x3f)>	Defines a TCP/UDP flag for the ACL.
reset	Resets the TCP/UDP parameters for the ACL to their default values.
cur	Displays the current TCP/UDP Filtering parameters.

## ACL Meter configuration

**Command:** /cfg/acl/acl <1-384>/meter

```
[Metering Menu]
  cir      - Set committed rate in KiloBits/s
  mbsize   - Set maximum burst size in KiloBits
  enable   - Enable/disable port metering
  dpass    - Set to Drop or Pass out of profile traffic
  reset    - Reset meter parameters
  cur      - Display current settings
```

This menu defines the metering profile for the selected ACL.

**Table 175** ACL Meter Configuration Menu options

Command	Description
cir <1000-10000000>	Configures the committed rate, in Kilobits per second. The committed rate must be a multiple of 1,000.
mbsize <32-4096>	Configures the maximum burst size, in Kilobits. Enter one of the following values for mbsize: 32, 64, 128, 256, 512, 1024, 2048, or 4096.
enable e d	Enables or disables metering on the ACL.
dpass drop pass	Configures the ACL Meter to either drop or pass out-of-profile traffic.
reset	Reset ACL Metering parameters to their default values.
cur	Displays the current ACL metering parameters.

## ACL Re-mark configuration

**Command:** /cfg/acl/acl <1-384>/re-mark

```
[Re-mark Menu]
  inprof   - In Profile Menu
  outprof  - Out Profile Menu
  reset    - Reset re-mark settings
  cur      - Display current settings
```

You can choose to re-mark IP header data for the selected ACL. You can configure different remark values, based on whether packets fall within the ACL Metering profile, or out of the ACL Metering profile.

**Table 176** ACL Re-mark Configuration Menu options

Command	Description
inprof	Displays the Re-mark In-Profile Menu.
outprof	Displays the Re-mark Out-of-Profile Menu.
reset	Reset ACL Re-mark parameters to their default values.
cur	Displays the current ACL re-mark parameters.

## ACL Re-mark In-Profile configuration

**Command:** /cfg/acl/acl <1-384>/re-mark/inprof

```
[Re-marking - In Profile Menu]
  uplp      - Set Update User Priority Menu
  updscp    - Set the update DSCP
  reset     - Reset in profile settings
  cur       - Display current settings
```

**Table 177** ACL Re-mark In-Profile Configuration Menu options

Command	Description
uplp	Displays the Re-Mark In-Profile Update User Priority Menu.
updscp <0-63>	Sets the DiffServ Code Point (DSCP) of In-Profile packets to the selected value.
reset	Resets the update DSCP parameters to their default values.
cur	Displays the current ACL re-mark in-profile parameters.

## ACL Re-mark In-Profile Update User Priority configuration

**Command:** /cfg/acl/acl <1-384>/re-mark/inprof/uplp

```
[Update User Priority Menu]
  value     - Set the update user priority
  utosp     - Enable/Disable use of TOS precedence
  reset     - Reset in profile uplp settings
  cur       - Display current settings
```

**Table 178** ACL Update User Priority Configuration Menu options

Command	Description
value <0-7>	Defines 802.1p value. The value is the priority bits information in the packet structure.
utosp enable disable	Enable or disable mapping of TOS (Type of Service) priority to 802.1p priority for In-Profile packets. When enabled, the TOS value is used to set the 802.1p value.
reset	Resets UP1P settings to their default values.
cur	Displays the current ACL Update User Priority parameters.

## ACL Re-mark Out-of-Profile configuration

**Command:** /cfg/acl/acl <1-384>/re-mark/outprof

```
[Re-marking - Out Of Profile Menu]
  updscp  - Set the update DSCP
  reset   - Reset out of profile settings
  cur     - Display current settings
```

**Table 179** ACL Re-mark Out-of-Profile Configuration Menu options

Command	Description
updscp <0-63>	Sets the DiffServ Code Point (DSCP) of Out-of-Profile packets to the selected value. The switch sets the DSCP value on Out-of-Profile packets.
reset	Resets the update DSCP parameters for Out-of-Profile packets to their default values.
cur	Displays the current ACL re-mark out-profile parameters.

## ACL Packet Format configuration

**Command:** /cfg/acl/acl <1-384>/pktfmt

```
[Filtering Packet Format Menu]
  ethfmt  - Set to filter on ethernet format
  tagfmt  - Set to filter on ethernet tagging format
  reset   - Reset all fields
  cur     - Display current parameters
```

The following table describes the Packet Format Configuration Menu options.

**Table 180** Packet Format Configuration Menu options

Command	Description
ethfmt eth2 snap llc	Defines the Ethernet format for the ACL.
tagfmt none tagged	Defines the tagging format for the ACL.
reset	Resets Packet Format parameters for the ACL to their default values.
cur	Displays the current Packet Format parameters for the ACL.

## ACL Group configuration

**Command:** `/cfg/acl/group <1-384>`

```
[ACL Group 1 Menu]
add      - Add ACL to group
rem      - Remove ACL from group
cur      - Display current ACL items in group
```

This menu allows you to compile one or more ACLs into an ACL Group. Once you create an ACL Group, you can assign the ACL Group to one or more ports.

The following table describes the ACL Group Configuration Menu options.

**Table 181** ACL Group Configuration Menu options

Command	Description
<code>add acl &lt;1-384&gt;</code>	Adds the selected ACL to the ACL Group. You can add up to 96 ACLs to each ACL Group.
<code>rem acl &lt;1-384&gt;</code>	Removes the selected ACL from the ACL Group.
<code>cur</code>	Displays the current ACL group parameters.

# Remote Monitoring configuration

**Command:** `/cfg/rmon`

```
[RMON Menu]
  hist      - RMON History Menu
  event     - RMON Event Menu
  alarm     - RMON Alarm Menu
  cur       - Display current RMON configuration
```

Remote Monitoring (RMON) allows you to monitor traffic flowing through the switch. The RMON MIB is described in RFC 1757.

The following table describes the RMON Configuration Menu options.

**Table 182** RMON Menu options

Command	Description
hist	Displays the RMON History Menu.
event	Displays the RMON Event Menu.
alarm	Displays the RMON Alarm Menu.
cur	Displays the current RMON configuration.

## RMON history configuration

**Command:** `/cfg/rmon/hist <1-65535>`

```
[RMON History 1 Menu]
  ifoid     - Set interface MIB object to monitor
  rbnum     - Set the number of requested buckets
  intrval   - Set polling interval
  owner     - Set owner for the RMON group of statistics
  delete    - Delete this history and restore defaults
  cur       - Display current history configuration
```

The following table describes the RMON History Menu options.

**Table 183** RMON History Menu options

Command	Description
ifoid <i>&lt;1-127 characters&gt;</i>	Configures the interface MIB Object Identifier. The IFOID must correspond to the standard interface OID, as follows: 1.3.6.1.2.1.2.2.1.1.x where x is the ifIndex (1-16, 18-21) The interface OID can have a maximum of 127 characters.
rbnum <i>&lt;1-65535&gt;</i>	Configures the requested number of buckets, which is the number of discrete time intervals over which data is to be saved. The range is from 1 to 65535. The default is 30. The maximum number of buckets that can be granted is 50.
intrval <i>&lt;1-3600&gt;</i>	Configures the time interval over which the data is sampled for each bucket. The range is from 1 to 3600 seconds. The default value is 1800 seconds.

**Table 183** RMON History Menu options

Command	Description
<code>owner &lt;1-127 characters&gt;</code>	Enter a text string that identifies the person or entity that uses this history index. The owner can have a maximum of 127 characters.
<code>delete</code>	Deletes the selected history index.
<code>cur</code>	Displays the current RMON History parameters.

## RMON event configuration

**Command:** `/cfg/rmon/event <1-65535>`

```
[RMON Event 1 Menu]
  descn  - Set description for the event
  type   - Set event type
  owner  - Set owner for the event
  delete - Delete this event and restore defaults
  cur    - Display current event configuration
```

The following table describes the RMON Event Menu options.

**Table 184** RMON Event Menu options

Command	Description
<code>descn &lt;1-127 characters&gt;</code>	Enter a text string to describe the event. The description can have a maximum of 127 characters.
<code>type none log trap both</code>	Selects the type of notification provided for this event. For log events, an entry is made in the log table and sent to the configured syslog host. For trap events, an SNMP trap is sent to the management station ( <code>/cfg/snmp/trap</code> ).
<code>owner &lt;1-127 characters&gt;</code>	Enter a text string that identifies the person or entity that uses this event index. The owner can have a maximum of 127 characters.
<code>delete</code>	Deletes this event index.
<code>cur</code>	Displays the current RMON Event parameters.



# RMON alarm configuration

**Command:** /cfg/rmon/alarm <1-65535>

```
[RMON Alarm 1 Menu]
oid      - Set MIB oid datasource to monitor
interval - Set alarm interval
sample   - Set sample type
almtypes - Set startup alarm type
rlimit   - Set rising threshold
flimit   - Set falling threshold
revtidx  - Set event index to fire on rising threshold crossing
fevtidx  - Set event index to fire on falling threshold crossing
owner    - Set owner for the alarm
delete   - Delete this alarm and restore defaults
cur      - Display current alarm configuration
```

The Alarm RMON group can track rising or falling values for a MIB object. The MIB object must be a counter, gauge, integer, or time interval. Each alarm index must correspond to an event index that triggers once the alarm threshold is crossed.

The following table describes the RMON Alarm Menu options.

**Table 185** RMON Alarm Menu options

Command	Description
oid <1-127 characters>	Configures an alarm MIB Object Identifier. The alarm OID can have a maximum of 127 characters.
interval <1-65535>	Configures the time interval over which data is sampled and compared with the rising and falling thresholds. The range is from 1 to 65535 seconds. The default is 1800 seconds.
sample abs delta	Configures the method of sampling the selected variable and calculating the value to be compared against the thresholds, as follows: <ul style="list-style-type: none"><li>• <b>abs</b>—absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval.</li><li>• <b>delta</b>—delta value, the value of the selected variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.</li></ul>
almtypes rising falling either	Configures the alarm type as rising, falling, or either (rising or falling).
rlimit <-2147483647 to 2147483647>	Configures the rising threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event is generated.
flimit <-2147483647 to 2147483647>	Configures the falling threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event is generated.

**Table 185** RMON Alarm Menu options

Command	Description
<code>revtidx &lt;0-65535&gt;</code>	Configures the rising alarm event index that is triggered when a rising threshold is crossed. The range is from 0 to 65535. The default value is 0.
<code>fevtidx &lt;0-65535&gt;</code>	Configures the falling alarm event index that is triggered when a falling threshold is crossed. The range is from 0 to 65535. The default value is 0.
<code>owner &lt;1-127 characters&gt;</code>	Enter a text string that identifies the person or entity that uses this alarm index. The owner can have a maximum of 127 characters.
<code>delete</code>	Deletes this alarm index.
<code>cur</code>	Displays the current RMON Alarm parameters.

## Port mirroring

**Command:** `/cfg/pmirr`

```
[Port Mirroring Menu]
mirror - Enable/Disable Mirroring
monport - Monitoring Port based PM Menu
cur      - Display All Mirrored and Monitoring Ports
```

The Port Mirroring Configuration Menu is used to configure, enable, and disable the monitored port. When enabled, network packets being sent and/or received on a target port are duplicated and sent to a monitor port. By attaching a network analyzer to the monitor port, you can collect detailed information about your network performance and usage. Port mirroring is disabled by default.

**NOTE:** See the “Troubleshooting tools” appendix in the *HP 10Gb Ethernet BL-c Switch Application Guide* for information on how to use port mirroring.

The following table describes the Port Mirroring Configuration Menu options.

**Table 186** Port Mirroring Configuration Menu options

Command	Description
<code>mirror disable enable</code>	Enables or disables port mirroring
<code>monport &lt;port number&gt;</code>	Displays port mirroring menu.
<code>cur</code>	Displays current settings of the mirrored and monitoring ports.

## Port-based port mirroring

**Command:** `/cfg/pmirr/monport <port number>`

```
[Port 1 Menu]
add      - Add "Mirrored" port
rem      - Rem "Mirrored" port
delete   - Delete this "Monitor" port
cur      - Display current Port-based Port Mirroring configuration
```

The following table describes the port-based Port Mirroring Configuration Menu options.

**Table 187** Port Mirroring Configuration Menu options

Command	Description
<code>add &lt;mirrored port&gt; in out both</code>	Adds the port to be mirrored. This command also allows you to enter the direction of the traffic. It is necessary to specify the direction because: <ul style="list-style-type: none"><li>• If the source port of the frame matches the mirrored port and the mirrored direction is ingress or both (ingress and egress), the frame is sent to the mirrored port.</li><li>• If the destination port of the frame matches the mirrored port and the mirrored direction is egress or both, the frame is sent to the monitoring port.</li></ul>
<code>rem &lt;mirrored port&gt;</code>	Removes the mirrored port.
<code>delete</code>	Deletes this monitored port.
<code>cur</code>	Displays the current settings of the monitoring port.

# Uplink Failure Detection configuration

**Command:** /cfg/ufd

```
[Uplink Failure Detection Menu]
  fdp - Failure Detection Pair Menu
  on  - Globally turn Uplink Failure Detection ON
  off - Globally turn Uplink Failure Detection OFF
  cur - Display current Uplink Failure Detection configuration
```

Uplink Failure Detection (UFD) supports network fault tolerance in network adapter teams. Use this menu to configure a Failure Detection Pair of one Links to Monitor (LtM) group and one Links to Disable (LtD) group. When UFD is enabled and a Failure Detection Pair is configured, the switch automatically disables ports in the LtD if it detects a failure in the LtM. The failure conditions which are monitored in the LtM group include port link state moving to down, or port state moving to Blocking if Spanning Tree Protocol is enabled.

The following table describes the Uplink Failure Detection (UFD) Configuration Menu options.

**Table 188** Uplink Failure Detection Configuration Menu options

Command	Description
fdp	Displays the Failure Detection Pair menu.
on	Globally turns Uplink Failure Detection ON.
off	Globally turns Uplink Failure Detection OFF.
cur	Displays the current Uplink Failure Detection configuration parameters.

## Failure Detection Pair configuration

**Command:** /cfg/ufd/fdp

```
[FDP Menu]
  ltm - Link to Monitor Menu
  ltd - Link to Disable Menu
  ena - Enable FDP
  dis - Disable FDP
  current - Display current FDP configuration
```

Use these commands to configure a Failure Detection Pair, which consists of one Link to Monitor (LtM) and one Link to Disable (LtD). When the switch detects a failure on the LtM, it automatically disables the ports in the LtD.

The following table describes the Failure Detection Pair (FDP) Configuration Menu options.

**Table 189** Failure Detection Pair Configuration Menu options

Command	Description
ltm	Displays the Links to Monitor menu.
ltd	Displays the Links to Disable menu.
ena	Enables the FDP Parameters.
dis	Disables the FDP Parameters.

**Table 189** Failure Detection Pair Configuration Menu options

Command	Description
current	Displays the current FDP configuration.

## Link to Monitor configuration

**Command:** /cfg/ufd/fdp/ltn

```
[Failure Link to Monitor Menu]
  addport - Add port to Link to Monitor
  remport - Remove port from Link to Monitor
  addtrnk - Add trunk to Link to Monitor
  remtrnk - Remove trunk from Link to Monitor
  addkey  - Add adminkey to Link to Monitor
  remkey  - Remove adminkey from Link to Monitor
  cur     - Display current LtM configuration
```

The following table describes the Link to Monitor (LtM) Menu options. The LtM can consist of only one uplink port (ports 18-21) or a single trunk containing only uplink ports.

**Table 190** Link to Monitor Menu options

Command	Description
addport <port number>	Adds a port to the LtM. Only uplink ports (18-21) are allowed in the LtM.
remport <port number>	Removes a port from the LtM.
addtrnk <1-12>	Adds a trunk group to the LtM. The LtM trunk group can contain only uplink ports (18-21).
remtrnk <1-12>	Removes a trunk group from the LtM.
addkey <1-65535>	Adds a LACP admin key to the LtM. LACP trunks formed with this admin key will be included in the LtM.
remkey <1-65535>	Removes a LACP admin key from the LtM.
cur	Displays the current LtM configuration.

## Link to Disable configuration

**Command:** /cfg/ufd/fdp/ltd

```
[Failure Link to Disable Menu]
  addport - Add port to Link to Disable
  remport - Remove port from Link to Disable
  addtrnk - Add trunk to Link to Disable
  remtrnk - Remove trunk from Link to Disable
  addkey  - Add adminkey to Link to Disable
  remkey  - Remove adminkey from Link to Disable
  cur     - Display current LtD configuration
```

The following table describes the Link to Disable (LtD) Menu options. The LtD can consist of any mix of downlink ports (ports 1-16) and trunk groups that contain only downlink ports.

**Table 191** Link to Disable Menu options

Command	Description
<code>addport &lt;port number&gt;</code>	Adds a port to the current LtD group. Only downlink ports (1-16) are allowed in the LtD.
<code>remport &lt;port number&gt;</code>	Removes a port from the current LtD group.
<code>addtrunk &lt;1-12&gt;</code>	Adds a trunk group to the current LtD group. LtD trunk groups can contain only downlink ports (1-16).
<code>remtrunk &lt;1-12&gt;</code>	Removes a trunk group from the current LtD group.
<code>addkey &lt;1-65535&gt;</code>	Adds a LACP admin key to the LtD. LACP trunks formed with this admin key will be included in the LtD.
<code>remkey &lt;1-65535&gt;</code>	Removes a LACP admin key from the LtD.
<code>cur</code>	Displays the current LtD configuration.

# Dump

**Command:** `/cfg/dump`

The dump program writes the current switch configuration to the terminal screen. To start the dump program, at the Configuration# prompt, enter:

```
Configuration# dump
```

The configuration is displayed with parameters that have been changed from the default values. The screen display can be captured, edited, and placed in a script file, which can be used to configure other switches. Paste the configuration commands from the script file at the command line prompt of the switch. The active configuration can also be saved or loaded via FTP/TFTP.

## Saving the active switch configuration

**Command:** `/cfg/ptcfg <FTP/TFTP server> <filename>`

When the `ptcfg` command is used, the active configuration commands of the switch (as displayed using `/cfg/dump`) will be uploaded to the specified script configuration file on the TFTP server. To start the switch configuration upload, at the Configuration# prompt, enter:

```
Configuration# ptcfg <FTP/TFTP server> <filename>
```

Where `<FTP/TFTP server>` is the FTP or TFTP server IP address or hostname and `<filename>` is the name of the target script configuration file.

---

**NOTE:** The output file is formatted with line-breaks but no carriage returns. The file cannot be viewed with editors that require carriage returns (such as Microsoft Notepad).

---

**NOTE:** If the TFTP server is running SunOS™ or the Solaris™ operating system, the specified `ptcfg` file must exist prior to executing the `ptcfg` command and must be writable (set with proper permission, and not locked by any application). The contents of the specified file will be replaced with the current configuration data.

---

## Restoring the active switch configuration

**Command:** `/cfg/gtcfg <FTP/TFTP server> <filename>`

When the `gtcfg` command is used, the active configuration will be replaced with the commands found in the specified configuration file. The file can contain a full switch configuration or a partial configuration. The configuration loaded using `gtcfg` is not activated until the `apply` command is used. If the `apply` command is found in the configuration script file loaded using this command, the `apply` action will be performed automatically.

To start the switch configuration download, at the Configuration# prompt, enter:

```
Configuration# gtcfg <FTP/TFTP server> <filename>
```

Where `<FTP/TFTP server>` is the FTP/TFTP server IP address or hostname and `<filename>` is the name of the target script configuration file.

---

**NOTE:** The switch supports three configuration files: active, backup, and factory. See the “Selecting a configuration block” section in the “Boot Options Menu” chapter for information on how to set which configuration file to use upon boot up.

---

---

# Operations Menu

## Introduction

Operations-level commands are used for making immediate and temporary changes to switch configuration. The Operations Menu is used for bringing ports temporarily in and out of service. This menu is available only from an administrator and operator login.

## Menu information

**Command:** `/oper`

```
[Operations Menu]
port      - Operational Port Menu
vrrp      - Operational Virtual Router Redundancy Menu
passwd    - Change current user password
clrlog    - Clear syslog messages
ntpreq    - Send NTP request
```

The following table describes the Operations Menu options.

**Table 192** Operations Menu options

Command	Description
<code>port &lt;port number&gt;</code>	Displays the Operational Port Menu.
<code>vrrp</code>	Displays the Operational Virtual Router Redundancy Menu.
<code>passwd &lt;1-128 characters&gt;</code>	Allows the user to change the password. You need to enter the current password in use for validation.
<code>clrlog</code>	Clears all Syslog messages.
<code>ntpreq</code>	Allows the user to send requests to the NTP server.

## Operations-level port options

**Command:** `/oper/port <port number>`

```
[Operations Port 1 Menu]
8021x     - 802.1x Menu
rmon      - Enable/Disable RMON for port
ena       - Enable port
dis       - Disable port
cur       - Current port state
```



Operations-level port options are used for temporarily disabling or enabling a port.

**Table 193** Operations-Level Port Menu options

Command	Description
8021x	Displays the 802.1X Port Menu.
rmon disable enable	Enables or disables Remote Monitoring for the port. RMON must be enabled for any RMON configurations to function.
ena	Temporarily enables the port. The port will be returned to its configured operation mode when the switch is reset.  This command does not enable a port that has been disabled by an ekeying mismatch error.
dis	Temporarily disables the port. The port will be returned to its configured operation mode when the switch is reset.
cur	Displays the current settings for the port.

## Operations-level port 802.1X options

**Command:** /oper/port <port number>/8021x

[802.1X Operation Menu]

- reset - Reinitialize 802.1X access control on this port
- reauth - Initiate reauthentication on this port now

Operations-level port 802.1X options are used to temporarily set 802.1X parameters for a port.

**Table 194** Operations-Level Port 802.1X Menu options

Command	Description
reset	Re-initializes the 802.1X access-control parameters for the port. The following actions take place, depending on the 802.1X port configuration: <ul style="list-style-type: none"><li>• force unauth—the port is placed in unauthorized state, and traffic is blocked.</li><li>• auto—the port is placed in unauthorized state, then authentication is initiated.</li><li>• force auth—the port is placed in authorized state, and authentication is not required.</li></ul>
reauth	Re-authenticates the supplicant (client) attached to the port. This command only applies if the port's 802.1X mode is configured as auto.

## Operations-level VRRP options

**Command:** `/oper/vrrp`

`[VRRP Operations Menu]  
back - Set virtual router to backup`

Operations-level VRRP options are described in the following table.

**Table 195** Operations-Level VRRP Menu options

Command	Description
<code>back &lt;1-255&gt;</code>	<p>Forces the specified master virtual router on this switch into backup mode. This is generally used for passing master control back to a preferred switch once the preferred switch has been returned to service after a failure. When this command is executed, the current master gives up control and initiates a new election by temporarily advertising its own priority level as 0 (lowest). After the new election, the virtual router forced into backup mode by this command will resume master control in the following cases:</p> <ul style="list-style-type: none"><li>• This switch owns the virtual router (the IP addresses of the virtual router and its IP interface are the same)</li><li>• This switch's virtual router has a higher priority and preemption is enabled.</li><li>• There are no other virtual routers available to take master control.</li></ul>

---

# Boot Options Menu

## Introduction

You must be logged in to the switch as the administrator to use the Boot Options Menu.

The Boot Options Menu provides options for:

- Selecting a switch software image to be used when the switch is next reset.
- Selecting a configuration block to be used when the switch is next reset.
- Downloading or uploading a new software image to the switch via FTP/TFTP.

## Menu information

**Command:** `/boot`

```
[Boot Options Menu]
  image - Select software image to use on next boot
  conf  - Select config block to use on next boot
  mode  - Select CLI mode to use on next boot
  prompt - Prompt for selectable boot mode
  gting - Download new software image via FTP/TFTP
  pting - Upload selected software image via FTP/TFTP
  reset - Reset switch [WARNING: Restarts Spanning Tree]
  cur   - Display current boot options
```

Each of the Boot Options Menu commands is discussed in greater detail in the following sections.

## Updating the switch software image

The switch software image is the executable code running on the switch. A version of the image ships with the switch, and comes pre-installed on the device. As new versions of the image are released, you can upgrade the software running on the switch.

Upgrading the software image on the switch requires the following:

- Loading the new image onto a FTP/TFTP server on your network
- Downloading the new image from the FTP/TFTP server to the switch
- Selecting the new software image to be loaded into switch memory the next time the switch is reset

## Downloading new software to the switch

The switch can store up to two different software images, called **image1** and **image2**, as well as boot software, called **boot**. When you download new software, you must specify where it should be placed: either into **image1**, **image2**, or **boot**.

For example, if your active image is currently loaded into **image1**, you would probably load the new image software into **image2**. This lets you test the new software and reload the original active image (stored in **image1**), if needed.

To download new software to the switch, you will need the following:

- The image or boot software loaded on a FTP or TFTP server on your network
- The hostname or IP address of the FTP or TFTP server
- The user name and password for FTP server, if necessary
- The name of the new software image or boot file

---

**NOTE:** The DNS parameters must be configured if specifying hostnames. See the “Domain name system configuration” section in the “Configuration Menu” chapter.

---

When the above requirements are met, use the following procedure to download the new software to your HP 10GbE switch.

1. At the Boot Options# prompt, enter:

```
Boot Options# gting
```

2. Enter the name of the HP 10GbE switch software to be replaced:

```
Enter name of switch software image to be replaced  
["image1"/"image2"/"boot"]: <image>
```

3. Enter the hostname or IP address of the FTP or TFTP server:

```
Enter hostname or IP address of FTP/TFTP server: <server name or IP  
address>
```

4. Enter the name of the new software file on the server:

```
Enter name of file on FTP/TFTP server: <filename>
```

The exact form of the name will vary by TFTP server. However, the file location is normally relative to the TFTP directory.

5. Enter the user name, if you are using a FTP server:

```
Enter username for FTP server or hit return for TFTP server: <userID>
```

6. Enter the password for the FTP server (if prompted):

```
Enter password for username on FTP server: <password>
```

7. Enter the port type to use for the file transfer:

```
Enter the port to use for downloading the image  
["mgt"|"data"]:
```

8. The system prompts you to confirm your request.

You should next select a software image to run, as described in the “Selecting a Soft Image to Run” section.

9. If you are loading an image from which you are not currently booted, the system prompts you to change the image.

```
image2 currently contains Software Version 1.0.1
that was downloaded at 15:46:36 Wed Mar 21, 2008.
New download will replace image2 with file "4.0.0_OS.img"
from TFTP server 10.168.2.4.
Confirm download operation [y/n]: y
Invoking TFTP over port 69...
Starting download...
File appears valid
Download in
progress.....
Image download complete (1333953 bytes)
Writing to flash...This takes about 90 seconds. Please wait
Write complete (1333953 bytes), now verifying FLASH...
Verification of new image2 in FLASH successful.
image2 now contains Software Version 4.0.0
Switch is currently set to boot software image1.
Do you want to change that to the new image2? [y/n] y
Next boot will use new software image2.
```

## Selecting a software image to run

You can select which software image (**image1** or **image2**) you want to run in switch memory for the next reboot.

1. At the Boot Options# prompt, enter:

```
Boot Options# image
```

2. Enter the name of the image you want the switch to use upon the next boot. The system informs you of which image is currently set to be loaded at the next reset, and prompts you to enter a new choice:

```
Currently set to use switch software "image1" on next reset.
Specify new image to use on next reset ["image1"/"image2"]:
```

## Uploading a software image from the switch

You can upload a software image from the switch to a FTP or TFTP server.

1. At the Boot Options# prompt, enter:

```
Boot Options# ptimg
```

2. The system prompts you for information. Enter the desired image:

```
Enter name of switch software image to be uploaded
["image1"|"image2"|"boot"]: <image> <hostname or server-IP-addr>
<server-filename>
```

3. Enter the name or the IP address of the FTP or TFTP server:

```
Enter hostname or IP address of FTP/TFTP server: <server name or IP
address>
```

4. Enter the name of the file into which the image will be uploaded on the FTP or TFTP server:

```
Enter name of file on FTP/TFTP server: <filename>
```

5. Enter the user name, if you are using a FTP server:

```
Enter username for FTP server or hit return for TFTP server: <userID>
```

6. Enter the password for the FTP server (if prompted):

```
Enter password for username on FTP server: <password>
```

7. The system then requests confirmation of what you have entered. To have the file uploaded, enter y.

```
image2 currently contains Software Version 4.0.0
Upload will transfer image2 (1889411 bytes) to file "test"
on TFTP server 10.1.1.1.
Confirm upload operation [y/n]: y
```

## Selecting a configuration block

When you make configuration changes to the switch, you must save the changes so that they are retained beyond the next time the switch is reset. When you execute the `save` command, your new configuration changes are placed in the active configuration block. The previous configuration is copied into the backup configuration block.

There is also a factory configuration block. This holds the default configuration set by the factory when the switch was manufactured. Under certain circumstances, it may be desirable to reset the switch configuration to the default. This can be useful when a custom-configured switch is moved to a network environment where it will be re-configured for a different purpose.

Use the following procedure to set which configuration block you want the switch to load the next time it is reset:

1. At the `Boot Options#` prompt, enter:

```
Boot Options# conf
```

2. Enter the name of the configuration block you want the switch to use.

The system indicates which configuration block is currently set to be loaded at the next reset, and prompts you to enter a new choice:

```
Currently set to use active configuration block on next reset.
Specify new block to use ["active"/"backup"/"factory"]:
```

## Resetting the switch

You can reset the switch to make your software image file and configuration block changes occur.

Resetting the switch causes the Spanning Tree Protocol to restart. This process can be lengthy, depending on the topology of your network.

To reset the switch, at the `Boot Options#` prompt, enter:

```
>> Boot Options# reset
```

You are prompted to confirm your request.

To display current boot options, enter:

```
>> Boot Options# cur
```

# Accessing the ISCLI

To access the ISCLI, enter the following command from the AOS CLI, and reset the switch:

```
Boot Options# mode iscli
```

The default command-line interface for the HP 10GbE switch is the AOS CLI. To access the AOS CLI, enter the following command and reset the switch:

```
>> Switch# boot cli-mode aos
```

Users can select the CLI mode upon login, if the `/boot/prompt` command is enabled. Only an administrator connected through the console port can view and enable `/boot/prompt`. When `/boot/prompt` is enabled, the first user to log in can select the CLI mode. Subsequent users must use the selected CLI mode, until all users have logged out.

# Maintenance Menu

## Introduction

The Maintenance Menu is used for debugging purposes, enabling you to generate a technical support dump of the critical state information in the switch, and to clear entries in the Forwarding Database and the Address Resolution Protocol (ARP) and routing tables. This menu is available only from an administrator and operator login.

## Menu information

**Command:** /maint

```
[Maintenance Menu]
  sys      - System Maintenance Menu
  fdb      - Forwarding Database Manipulation Menu
  debug    - Debugging Menu
  arp      - ARP Cache Manipulation Menu
  route    - IP Route Manipulation Menu
  igmp     - IGMP Multicast Group Menu
  uudmp    - Uuencode FLASH dump
  ptdmp    - Upload FLASH dump via FTP/TFTP
  ptfile   - Upload FLASH dump via FTP/TFTP
  cldmp    - Clear FLASH dump
  panic    - Dump state information to FLASH and reboot
  tsdmp    - Tech support dump
  pttsdmp  - Upload tech support dump via FTP/TFTP
```

Dump information contains internal switch state data that is written to flash memory on the switch after any one of the following occurs:

- The switch administrator forces a switch panic. The panic option, found in the Maintenance Menu, causes the switch to dump state information to flash memory, and then causes the switch to reboot.
- The switch administrator enters the switch reset key combination (**Ctrl-Shift-6**) on a device that is attached to the console port.
- The switch detects a hardware or software problem that requires a reboot.

The following table describes the Maintenance Menu options.

**Table 196** Maintenance Menu options

Command	Usage
sys	Displays the System Maintenance Menu.
fdb	Displays the Forwarding Database Manipulation Menu.
debug	Displays the Debug Menu.
arp	Displays the ARP Cache Manipulation Menu.
route	Displays the IP Route Manipulation Menu.



**Table 196** Maintenance Menu options

Command	Usage
igmp	Displays the IGMP Maintenance Menu.
uudmp	Displays dump information in uuencoded format.
ptdmp	Saves the system dump information via FTP/TFTP.
ptfile	Saves a specified file from the switch root file system to an FTP/TFTP server.
cltmp	Clears dump information from flash memory.
panic	Dumps MP information to flash and reboots.
tsdmp	Dumps all switch information, statistics, and configuration.
pttsdmp	Redirects the technical support dump (tsdmp) to an external FTP/TFTP server.

## System maintenance options

**Command:** /maint/sys

```
[System Maintenance Menu]
flags - Set NVRAM flag word
```

The System Maintenance Menu is reserved for use by HP technical support. The options are used to perform system debugging.

The following table describes the System Maintenance Menu options.

**Table 197** System Maintenance Menu options

Command	Usage
<code>flags &lt;new NVRAM flags word as 0XXXXXXXX&gt;</code>	Sets the flags that are used for debugging purposes by HP technical support.

## Forwarding Database options

**Command:** /maint/fdb

```
[FDB Manipulation Menu]
  find      - Show a single FDB entry by MAC address
  port      - Show FDB entries for a single port
  vlan      - Show FDB entries for a single VLAN
  dump      - Show all FDB entries
  clear     - Clear entire FDB, then re-add static entries
```

The Forwarding Database (FDB) Manipulation Menu can be used to view information and to delete a MAC address from the Forwarding Database or clear the entire Forwarding Database. This is helpful in identifying problems associated with MAC address learning and packet forwarding decisions.

The following table describes the FDB Manipulation Menu options.

**Table 198** FDB Manipulation Menu options

Command	Usage
<code>find &lt;MAC address&gt; [&lt;1-4094&gt;]</code>	Displays a single database entry by its MAC address. You are prompted to enter the MAC address of the device. Enter the MAC address using one of the following: <ul style="list-style-type: none"><li>• <code>xx:xx:xx:xx:xx:xx</code> format (for example: 08:00:20:12:34:56)</li><li>• <code>xxxxxxxxxxxx</code> format (for example: 080020123456)</li></ul>
<code>port &lt;port number&gt;</code>	Displays all FDB entries for a particular port.
<code>vlan &lt;1-4094&gt;</code>	Displays all FDB entries on a single VLAN.
<code>dump</code>	Displays all entries in the Forwarding Database.
<code>clear</code>	Clears the entire Forwarding Database from switch memory, and then adds the static entries to the Forwarding Database.

## Debugging options

**Command:** /maint/debug

```
[Miscellaneous Debug Menu]
  tbuf      - Show MP trace buffer
  snap      - Show MP snap (or post-mortem) trace buffer
  clrcfg    - Clear all flash configs
```

The Miscellaneous Debug Menu displays trace buffer information about events that can be helpful in understanding switch operation. You can view the following information using the Debug Menu:

- Events traced by the management processor (MP)
- Events traced to a buffer area when a reset occurs

If the switch resets for any reason, the management processor (MP) trace buffer is saved into the snap trace buffer area. The output from these commands can be interpreted by HP technical support.

The following table describes the Miscellaneous Debug Menu options:

**Table 199** Miscellaneous Debug Menu options

Command	Usage
tbuf	Displays the management processor trace buffer. Header information similar to the following is shown: MP trace buffer at 13:28:15 Fri May 25, 2002; mask: 0x2ffdf748 The buffer information is displayed after the header.
snap	Displays the management processor snap (or post-mortem) trace buffer. This buffer contains information traced at the time that a reset occurred.
clrcfg	Deletes all flash configuration blocks. The next time the switch is rebooted, it returns to the factory default settings.

## ARP cache options

**Command:** /maint/arp

```
[Address Resolution Protocol Menu]
  find    - Show a single ARP entry by IP address
  port    - Show ARP entries on a single port
  vlan    - Show ARP entries on a single VLAN
  addr    - Show ARP entries for switch's interfaces
  dump    - Show all ARP entries
  clear   - Clear ARP cache
```

The following table describes the Address Resolution Protocol Menu options:

**Table 200** Address Resolution Protocol Menu options

Command	Usage
find <IP address>	Shows a single ARP entry by IP address. For example, 192.4.17.35.
port <port number>	Shows ARP entries on a single port.
vlan <1-4094>	Shows ARP entries on a single VLAN.
addr	Shows the list of IP addresses that the switch will respond to for ARP requests.
dump	Shows all ARP entries.
clear	Clears the entire ARP list from switch memory.

**NOTE:** To display all ARP entries currently held in the switch, or a portion according to one of the options listed on the menu above (find, port, vlan, dump), see the “ARP information” section of the “Information Menu” chapter.

## IP Route Manipulation options

**Command:** /maint/route

```
[IP Routing Menu]
  find      - Show a single route by destination IP address
  gw        - Show routes to a single gateway
  type      - Show routes of a single type
  tag       - Show routes of a single tag
  if        - Show routes on a single interface
  dump      - Show all routes
  clear     - Clear route table
```

The following table describes the IP Route Manipulation Menu options:

**Table 201** IP Route Manipulation Menu options

Command	Usage
find <IP address>	Shows a single route by destination IP address.
gw <IP address>	Shows routes to a default gateway.
type indirect direct local broadcast martian multicast	Shows routes of a single type.
tag fixed static addr rip ospf broadcast martian	Shows routes of a single tag.
if <1-250>	Shows routes on a single interface.
dump	Shows all routes.
clear	Clears the route table from switch memory.

## IGMP Multicast Group options

**Command:** /maint/igmp

```
[IGMP Multicast Group Menu]
  snoop      - IGMP Snooping Menu
  mrouter    - IGMP Multicast Router Port Menu
  clear      - Clear group and mrouter tables
```

The following table describes the IGMP Multicast Group Maintenance Menu options.

**Table 202** IGMP Multicast Group Menu options

Command	Usage
snoop	Displays the IGMP Snooping maintenance menu.
mrouter	Displays the IGMP Multicast Router maintenance menu.
clear	Clears IGMP Multicast data from switch memory.

## IGMP Snooping options

**Command:** /maint/igmp/snoop

```
[IGMP Multicast Group Menu]
  find      - Show a single group by IP group address
  vlan      - Show groups on a single vlan
  port      - Show groups on a single port
  trunk     - Show groups on a single trunk
  detail    - Show detail of a single group by IP address
  dump      - Show all groups
  clear     - Clear group tables
```

The following table describes the IGMP Snoop Maintenance Menu options.

**Table 203** IGMP Snooping Menu options

Command	Usage
find <IP address>	Shows a single IGMP Multicast group by IP address.
vlan <1-4094>	Shows IGMP Multicast groups on a single VLAN.
port <port number>	Shows IGMP Multicast groups on a single port.
trunk <1-40>	Displays all IGMP multicast groups on a single trunk group. (To be added-LACP trunks)
detail <IP address>	Displays details about IGMP multicast groups, including source and timer information.
dump	Shows all IGMP Multicast groups.
clear	Clears IGMP Multicast data from switch memory.

## IGMP Mrouter options

**Command:** /maint/igmp/mrouter

```
[IGMP Multicast Routers Menu]
  vlan      - Show all multicast router ports on a single vlan
  dump      - Show all multicast router ports
  clear     - Clear multicast router port table
```

The following table describes the IGMP Multicast Routers Maintenance Menu options.

**Table 204** IGMP Multicast Group Menu options

Command	Usage
vlan <1-4094>	Shows IGMP Multicast groups on a single VLAN.
dump	Shows all IGMP Multicast routers.
clear	Clears IGMP Multicast router data from switch memory.

## Uencode flash dump

**Command:** /maint/uudmp

Using this command, dump information is presented in uuencoded format. This format makes it easy to capture the dump information as a file or a string of characters.

If you want to capture dump information to a file, set your communication software on your workstation to capture session data prior to issuing the `uudmp` command. This will ensure that you do not lose any information. Once entered, the `uudmp` command will cause approximately 23,300 lines of data to be displayed on your screen and copied into the file.

Using the `uudmp` command, dump information can be read multiple times. The command does not cause the information to be updated or cleared from flash memory.

Dump information is not cleared automatically. In order for any subsequent dump information to be written to flash memory, you must manually clear the dump region. For more information on clearing the dump region, see the “Clearing dump information” section later in this chapter.

To access dump information, at the Maintenance# prompt, enter:

```
Maintenance# uudmp
```

The dump information is displayed on your screen and, if you have configured your communication software to do so, captured to a file. If the dump region is empty, the following displays:

```
No FLASH dump available.
```

## FTP/TFTP system dump put

**Command:** /maint/ptdmp <server> <filename>

Use this command to put (save) the system dump to a FTP or TFTP server.

**NOTE:** If the FTP/TFTP server is running SunOS or the Solaris operating system, the specified `ptdmp` file must exist prior to executing the `ptdmp` command, and must be writable (set with proper permission, and not locked by any application). The contents of the specified file will be replaced with the current dump data.

To save dump information via FTP/TFTP, at the Maintenance# prompt, enter:

```
Maintenance# ptdmp <server> <filename>
```

Type the FTP/TFTP server IP address or hostname as <server>, and the target dump file as <filename>. You are prompted to choose the port type (data port or management port) to use for the file transfer.

## Clearing dump information

**Command:** /maint/cltmp

To clear dump information from flash memory, at the Maintenance# prompt, enter:

```
Maintenance# cltmp
```

The switch clears the dump region of flash memory and displays the following message:

```
FLASH dump region cleared.
```

If the flash dump region is already clear, the switch displays the following message:

```
FLASH dump region is already clear.
```

## Panic command

**Command:** /maint/panic

The panic command causes the switch to immediately dump state information to flash memory and automatically reboot.

To select panic, at the Maintenance# prompt, enter:

```
>> Maintenance# panic
A FLASH dump already exists.
Confirm replacing existing dump and reboot [y/n]:
```

Enter y to confirm the command:

```
Confirm dump and reboot [y/n]: y
```

A list of messages is displayed:

```
Starting system dump...done.

Reboot at 11:54:08 Wednesday March 21, 2008...

. . . . .

. . . . .

Rebooted because of console PANIC command.

Booting complete
```

## Unscheduled system dumps

If there is an unscheduled system dump to flash memory, the following message is displayed when you log on to the switch:

```
Note: A system dump exists in FLASH. The dump was saved
      at 13:43:22 Wednesday March 21, 2008. Use /maint/uudmp to
      extract the dump for analysis and /maint/cltmp to
      clear the FLASH region. The region must be cleared
      before another dump can be saved.
```

---

# Index

## 8

802.1x information, 40

802.1x statistics, 74

## A

abbreviating commands, 18

access control, user, 125

active configuration block, 110, 214

active switch configuration

    gtcfg, 207

    ptcfg, 207

    restoring, 207

Address Resolution Protocol (ARP)

    address list, 219

Address Resolution Protocol (ARP) Menu, 53

aging

    STP information, 43, 45

apply command, 15, 109

auto-negotiation

    enable/disable on port, 133

    flow control configuration, 133

## B

backup configuration block, 110, 214

banner (system option), 112

Boot Options Menu, 211

bootstrap protocol (BOOTP)

    obtain the IP address, 9

BPDU guard

    configuration, 135

bridge maximum age parameter

    configuration, 145

    information, 43, 45, 47

bridge parameter menu, for STP, 141

bridge priority, 43

Bridge Protocol Data Unit (BPDU), 43, 45, 47

bridge Spanning Tree parameters, 145

## C

capture dump information to a file, 222

clear

    ARP entries, 219

    dump information, 222

commands

    abbreviations, 18

    global commands, 15

    shortcuts, 18

    tab completion, 18

Common Internal Spanning Tree information, 46

configuration

    apply changes, 109

    default gateway interval, for health checks, 160

    default gateway IP address, 160

    dump command, 207

    flow control, 133

    Gigabit Ethernet, 131

    operating mode, 133

    port mirroring, 202

    port trunking, 149

    revert changes, 109

    save changes, 110

    switch IP address, 159

    view pending changes, 109

    VLAN default (PVID), 131

    VLAN IP interface, 159

    VLAN tagging, 131

configuration block, 214

configuring RMON (remote monitoring), 199

connecting

    via console, 9

    via Secure Shell (SSH), 10

    via Telnet, 10

console port, connecting, 9

cost

    STP information, 43, 45, 47

    STP port option, 147

## D

debugging, 216

default gateway, interval for health checks, 160

default password

    administrator, 20

    operator, 22



- user, 22
- diff command, 15, 109
- diff flash command, 15, 109
- disconnect idle timeout, 12
- download software, 211
- dump
  - configuration, 207
  - information, 71
  - state information, 223
  - statistics, 107
- duplex mode, link status, 24, 69
- dynamic routes, 220

**F**

- factory configuration block, 214
- factory default configuration, 19
- first-time configuration, 19
- flow control
  - configuration, 133
  - display setting, 24
  - link status, 69
- Forwarding Database (FDB)
  - maintenance, 218
- Forwarding Database Information Menu, 37
- Forwarding Database Manipulation Menu, 218
- forwarding state (FWD), 38, 43, 45, 47, 48
- fwd (STP bridge option), 146
- FwdDel (forward delay), bridge port, 43, 45, 47

**G**

- gig (Port Menu option), 131
- Gigabit Ethernet Physical Link, 131
- Gigabit Ethernet, configuration, 131
- global commands, 15
- gtcfg (TFTP load command), 207

**H**

- health checks
  - default gateway interval, retries, 160
  - retry, number of failed health checks, 160
- hello, STP information, 43, 45, 47
- history command, 16
- Hot Links
  - configuration, 155

**I**

- idle timeout, overview, 12
- IEEE standards, 802.1d Spanning Tree Protocol, 42

- IGMP Mrouter options, 221
- IGMP Multicast Group options, 220
- IGMP Snooping options, 221
- IGMPv3
  - configuration, 177
- image
  - download, 211
  - software, selection, 213
- information dump, 71
- Information Menu, 24
- interface statistics, 79, 81
- Internet Protocol (IP) statistics, 81
- IP address
  - ARP information, 53
  - BOOTP, 9
  - default gateway configuration, 160
- active IP interface
  - active, 188
- IP interface
  - address configuration, 159
  - information, 59
  - VLAN configuration, 159
- IP Interface Configuration Menu, 159
- IP Route Manipulation options, 220

**L**

- LACP statistics, 84
- Layer 2 information, 36
- Layer 2 statistics, 84
- Layer 3 information, 50
- Layer 3 statistics, 86
- LEARNING (port state), 43, 45, 47
- lines command, 15
- Link Aggregation Control Protocol information, 38
- link status
  - command, 69
  - display setting, 24
  - duplex mode, 24, 69
  - port speed, 24, 69
- log, syslog messages, 113
- login notice, 112

**M**

- Main Menu, 14
- Maintenance Menu, 216
- management processor (MP)
  - trace buffer, 218

- mask, IP interface subnet address, 159
- MD5 cryptographic authentication, 169
- media access control (MAC) address
  - ARP information, 53
  - display address, 9
  - FDB information, 37
  - FDB manipulation, 218
- Miscellaneous Debug Menu, 218
- monitor port, 202

## N

- Network Time Protocol (NTP)
  - synchronization, 118
- null modem cable, 9
- online help, 15
- operating mode, configuration, 133
- Operations-level port 802.1x options, 209
- Operations-level port options, 208
- Operations-level VRRP options, 210
- ospf
  - area index, 168
  - interface, 168
  - Not-So-Stubby Area, 169
  - stub area, 169
  - transit area, 169
- OSPF configuration, 168
- OSPF information, 54

## P

- panic
  - command, 223
  - switch, 216
- passwords, defaults, 20
- ping command, 16
- popd command, 16
- port configuration, 131
- Port Menu
  - configuration options, 132, 133, 134
  - Gigabit Ethernet (gig) configuration, 131
- port mirroring, configuration, 202
- port number, 69
- port speed, 24, 69
- port statistics, 73
- port trunking configuration, 149
- ports
  - disable (temporarily), 132

- information, 70
- membership of the VLAN, 49
- priority, 43, 45, 47
- STP port priority, 147
- preemption
  - assuming VRRP master routing authority, 185
- priority (STP port option), 147
- prisrv, primary radius server, 115
- Private VLAN
  - configuration, 154
- Protocol VLAN
  - configuration, 153
- ptcfg (TFTP save command), 207
- pushd command, 16
- pwd command, 16

## Q

- quiet (screen display option), 16

## R

- Rapid Spanning Tree and Multiple Spanning Tree information, 44
- read community string (SNMP option), 119
- reboot, 216, 223
- retries, radius server, 115
- retry, health checks for default gateway, 160
- revert apply command, 16, 109
- revert command, 16, 109
- RMON
  - alarm information, 67
  - event information, 68
  - history information, 66
- RMON configuration
  - alarm, 201
  - event, 200
  - history, 199
- RMON Information Menu, 66
- poisoned reverse, as used with split horizon
  - poisoned reverse, 166
- Routing Information Protocol (RIP)
  - version 1 parameters, 162, 165, 166
- split horizon
  - split horizon, 166
- save command, 16, 110, 214
- save n command, 16
- secret, radius server, 115

## S

- secsrv, secondary radius server, 115
- Secure Shell (SSH)
  - encryption and authentication methods, 10
- Secure Shell Server (SSHD) Menu, 114
- Server Mobility
  - configuration, 181
- Setup utility
  - introduction, 19
  - start, 19
- shortcuts, 18
- Simple Network Management Protocol (SNMP)
  - optional setup, 20
- snap traces, buffer, 218
- SNMP
  - set and get access, 120
- SNMPv3 Access Table information, 28
- SNMPv3 Community Table information, 29
- SNMPv3 dump, 32
- SNMPv3 Group Table information, 29
- SNMPv3 Information Menu, 26
- SNMPv3 Notify Table information, 31
- SNMPv3 Target Address Table information, 30
- SNMPv3 Target Parameters Table information, 30
- SNMPv3 USM User Table information, 27
- SNMPv3 View Table information, 27
- software
  - image, 211
- Spanning Tree Protocol (STP)
  - bridge parameters, 145
  - information, 42
  - port cost option, 147
  - port priority option, 147
  - root bridge, 145
  - switch reset effect, 214
  - with trunk groups, 48
- sshport, 114
- starting switch setup, 19
- state (STP information), 43, 45, 47
- statistics dump, 107
- Statistics Menu, 72
- subnet address mask configuration, IP subnet address, 159
- subnets
  - IP interface, 159
- switch
  - reset, 214

- syslog
  - display messages, 34
- system
  - date and time, 25, 26, 27, 28, 29, 30, 31, 35, 36, 50, 84
  - information, 33, 71
- System Configuration Menu, 111
- System Information Menu, 25
- system options
  - login banner, 112
  - tnport, 112

## T

- tab completion, 18
- TCP statistics, 100, 101
- Telnet
  - requirements, 10
- telnet command, 16
- timeout, radius server, 115
- timeouts, idle connection, 12
- tnport, system option, 112
- trace buffer, 218
- traceroute command, 16
- Tracking
  - VRRP
    - tracking, 184
- transmit flow control, 133
- Trivial File Transfer Protocol (TFTP)
  - PUT and GET commands, 207
  - use for updating switch software image, 211
- typographical conventions, 13

## U

- UCB statistics, 101
- UDP statistics, 93
- unscheduled system dump, 223
- upgrade, switch software, 211
- user access control configuration, 125
- user access levels, 11
- uuencode flash dump, 222

## V

- verbose n command, 16
- view pending configuration changes, 109
- virtual router
  - description, 184
  - tracking criteria, 185
- virtual router group

- VRRP priority tracking, 187
- Virtual Router Redundancy Protocol (VRRP)
  - password, authentication
    - VRRP authentication, 188
  - group options (prio)
    - virtual router
      - priority, 187
  - priority election for the virtual router, 185
- virtual routers
  - increasing priority level of, 185
  - master preemption (preem)
    - virtual router, 187
  - master preemption (prio)
    - virtual router, 185
- VLAN
  - active port
    - VLAN, 188
- VLAN tagging

- port configuration, 131
- VLANs
  - ARP entry information, 53
  - configuration, 152
  - information, 49
  - name, 49
  - port membership, 49
  - setting default number (PVID), 131
  - tagging, 25, 70
  - VLAN number, 49
- VRID (virtual router ID), 184, 187
- VRRP
  - master advertisements, 185
- VRRP configuration, 183
- VRRP information, 62
- VRRP master advertisements
  - time interval, 187
- VRRP statistics menu, 98